



## Privacy and Security Sub Work Group Agenda

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

Topic 1:	Housekeeping and Logistics <b>Roll Call of Voting Members</b> <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> <b>Approval of meeting minutes</b> <b>Review of Meeting Schedule- timeline</b> <b>Questions</b>
Topic 2:	Review of draft policies <ul style="list-style-type: none"> <li>• <b>Access</b></li> <li>• <b>Authorization</b></li> <li>• <b>Authentication</b></li> </ul>
Topic 3:	Strategic Plan <b>Please continue to review updated versions and make comments on Work Zone</b>
Topic 4:	Next Meeting Reminder Tuesday, March 16, 9-11 am



## Privacy and Security Sub Work Group Meeting Minutes

<b>Meeting Date:</b>	Tuesday Feb 23, 2010	<b>Facilitator:</b>	Kelly Coyle
<b>Place:</b>	Web-ex	<b>Web-ex Information:</b>	<a href="https://premconf.webex.com/premconf/j.php?ED=102879222&amp;UID=0">https://premconf.webex.com/premconf/j.php?ED=102879222&amp;UID=0</a> password: mihin-ps5
<b>Time:</b>	9:00 – 11:00 AM	<b>Teleconference #:</b>	1-888-3948197 passcode 869479

Topic 1:	<p>Housekeeping and Logistics</p> <p><b>Roll Call of Voting Members</b> <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></p> <p><b>Approval of meeting minutes</b> <b>State HIE Announcement</b> <b>Review of Meeting Schedule- timeline</b> <b>Google Groups Update</b> <b>Questions</b></p>
Topic 2:	<p><b>Finish Up Consent/VOTE</b></p> <p>Presentation Discussion VOTE on Individual Consent Option Policy Requirements Opt Out Form:Review</p>
Topic 3:	<p>Next Meeting Reminder</p> <p style="text-align: center;"><b>Tuesday, March 9, 9-11 am</b></p>

DISCUSSION	Topic 1: <b>Housekeeping and Logistics</b>
------------	--

**Roll Call of Voting Members:** All voting members are present except for George Goeble and Nancy Walker

**Approval of meeting minutes:**

MOTION: Approve meeting minutes

MOTION SECONDED

VOTE: Approved (all present Voting Members)

ACTION ITEMS	PERSON RESPONSIBLE	DEADLINE
None.		

DISCUSSION	Topic 2: <b>Finish Up Consent/VOTE</b>
------------	--

- a. Beth Nagel presented an overview of the State HIE Announcement.
- b. Kelly requested a motion to rescind the last two motions voted on at the last meeting as they seem to take us back to opt in.

- a. A voting member stated his perception of that motion was that a provider would obtain an NPP once and that would allow retrieval of the data for that patient. Kelly and Denise confirmed that this is the point of confusion as the motion as stated otherwise.
  - b. Comments are made that sharing and retrieval are two different components that might work differently and there is confusion over how it would work technically versus what the group needs to do to establish a policy.
  - c. The group has already decided we are not doing consent to get data into the HIE and what we are now talking about is all patients' data being in the HIE but access to ~~to~~ the data by other providers being restricted.
  - d. Motion to rescind is made. Discussion followed regarding interpretation of the prior motion. Voting members agree to rescind the motion.
- c. Discussion follows:
- a. A voting member asks that since the backbone is a conduit (not storage) we are talking about whether data is retained or purged at the HIE, correct? Kelly agrees and adds that if the backbone has minimum policies, the HIEs can have more stringent policies and HIEs may need guidance that can be supplied at the State level. The voting member points out that many HIEs are themselves conduits, with data not stored at the HIE level.
  - b. Another member comments that data should never be purged (policy is to retain data for at least 7 yrs or until age of majority) and adds that another reason to not purge data is in case of a mismatch. Clarification made that we really aren't talking about "purging" data – we are talking about the data not being entered into the MiHIN at all.
  - c. Another voting member points out that we should remind ourselves that many large health systems that already do business with electronic medical records so some of the concerns may not an issue in those situations.
  - d. Kelly reminds everyone that consent needs to be looked at holistically – there are other pieces that come into play – authorization, authentication, access, and audit. We will be addressing the 4 A's in addition to the consent issues we have been discussing.
- d. ~~Kelly suggests~~ Kelly suggests that a voting ~~member make~~ member make a motion that states that data will be retained and restricted by all Community HIEs when an individual opts out of sharing all their data or a limited class of data.
- a. Mike comments that this motion needs to be stronger because as worded, this motion allows HIEs to "do their own thing" and could result in an HIE not being able to connect in to everything else. The standards for an HIE to participate in the MiHIN need to be clear.
  - b. This triggers another comment about HIEs being conduits of data rather than providing storage of data and if there are additional capabilities needed to fulfill additional requirements, the HIEs might not be able to comply without assistance and resources to help them adapt.
  - c. Kelly suggests that guidance along these lines to the HIEs will be great value but the group has to be reasonable and set minimums. This will save the HIEs time and money and they can have their own more stringent regulations, understanding that more stringent regulations could mean they are not be able to send/share within the MiHIN.
  - d. Several members prefer the motion to say that if the opted-out data is retained at the HIE, access to it will be restricted.
- e. Melissa sends a motion that reads "An opt-out decision affects the ability to disclose the data to other healthcare providers, rather than the ability to transmit data to the HIE, and that any data transmitted to the HIE which is subject to an opt-out decision may be retained, but access shall be restricted."
- a. Comment made that when a person opts out, they will think the data is not out there *at all and there will be no risk of breach*. Education is very important and it must be very consistent through the state.
  - b. Kelly adds that data is currently out there now. Have to remember that audits are happening now, a privacy officer has been appointed by the ONC and education materials will be made available. Emphasize that just because data is electronic, it doesn't mean that it will be shared differently than now. Benefits should outweigh the negatives.
  - c. Comment made that we should be concerned about the 1% or less that end up in lawsuits. Incomplete opt-out is risky for providers and education would not counter that. Without state law requiring ~~that~~ providers to forward data to this network, thinks there's a great risk if patients don't have opportunity to completely opt out and not have data there at all. While the risk is already there and yes, the data might go somewhere it shouldn't, the reality is that all will be electronic and the ability of a provider to keep an individual patient's data on paper will not be feasible.

- d. Discussion on whether specially protected health information should be treated differently, i.e., not allowed to flow into HIE – no. All information should flow into the HIE and all would be restricted Categories of protected information could be tagged so they are not passed but individual pieces of information are difficult to tag. The law protects certain information and the special consent required by law will continue to be necessary to access that information..
- e.
- f. Kelly reiterates – when you see a provider and they present NPP and you sign, you are agreeing that the provider share your info – you don’t get to pick and chose as to how they share it. Consent is implied - yes we will retain the data, yes it will be electronic, the choice the patient gets to make is the decision that the data cannot be accessed via the MiHIN.
- f. The motion is: That community HIEs may retain and restrict disclosure of data upon the patient’s request to opt-out. Restrictions may be limited to certain types of data subject to more-restrictive legal requirements.
- a) Discussion ensues on whether the HIE can leave the data out. ~~Yes-Question~~ Yes. Question jurisdiction of this group – if we’re setting policy for HIEs, can the opt-out be a function of the backbone? Don’t want to have to opt out of every HIE. Mike explained a procedural mechanism could allow opt out once. Backbone will know what community HIE policies are and then can restrict based on those policies. Each HIE will have to manage own consent and make own decisions on how. Comment made that it’s a burden on the HIE to manage these types of policies/procedures – there will have to be a subsidy from the state to cover the burden of these technical and management issues.
- b) Can’t have situations where people want to opt-out of particular data that is not restricted by law.
- c) Group is ~~reminded that~~ reminded that since a paper process is not in our futures, will opt-out decisions even be indulged?
- d) There is a vote and all approve the motion as follows:  
 That an "opt-out" decision affects the ability to disclose the data to other healthcare providers, rather than the ability to transmit data to the HIE, and that any data transmitted to the HIE which is subject to an opt-out decision may be retained, but access shall be restricted. Data which is subject to legally-imposed special restrictions will be used and/or disclosed in accordance with law.
- e) Education will be paramount so that the public knows what “Opt Out” means
- g) Kelly moves on to the next set of options to be discussed. What opt out options will the patient have? - Where patient does nothing, special consent is still needed for specially protected info. If a patient has opted-out, that information will not be shared except in emergency situations. At all times the doctor would need special consent to get access to specially protected information. There will be a screen that will require the provider to acknowledge that they have a treatment relationship with the patient and if the data requested is specially protected health information under law, the provider has obtained the special consent required by law. .
- a. Again education will be critical.
- b. Discussion re: what opt out versuse opt out with exceptions really means.
- c. The group is on the same page conceptually but the language that has been chosen needs to be clearer.

ACTION ITEMS	PERSON RESPONSIBLE	DEADLINE
None.		

Attendees:

- David Allen                      MiHIN PCO – Consulting Team
- George Boersma                MiHIN PCO
- Jeff Bontsas                      Voting Member
- Don Carne                        Member
- Denise Chrylser                 Voting Member
- Kathleen Cornish                MPHI
- Moira Davenport-Ash            Voting Member
- Darrell Dontje                    Voting Member
- Chuck Dougherty                Voting Member
- Cynthia Edwards                Member
- Mike Gagnon                      MiHIN PCO – Consulting Team



- Harlan Goodrich Member
- Violand Grigorescu Member
- John Hazewinkel Voting Member
- Guy Hembroff Member
- Huzaifa Jamali MiHIN PCO – Consulting Team
- Michael Khoury Member
- Pat Klima Member
- Glen Lutz Voting Member
- Linda McCardel MPHI
- Troy Lane Member
- Harry Levins MPHI
- Glen Lutz Voting Member
- Pat Maltby MiHIN PCO
- Margaret Marchak Chairperson
- Melissa Markey Voting Member
- Linda McCardel MPHI
- Robert Moerland Member
- Teresa Mulford Member
- Paul Muneio Member
- Amber Murphy MiHIN PCO – Consulting Team
- Beth Nagel MiHIN PCO
- Harvey Organek Member
- Kurt Riegel Member
- Kim Roberts Member
- Mick Talley Member
- Stewart Tan General Public
- Mike Tarn Voting Member
- Shelli Weisberg Voting Member

## MiHIN Access Policy

Access controls govern when and how a patient's information may be accessed by authorized individuals within a Community HIE's Participant. These access policies, coupled with informed patient consent, are designed to reduce unauthorized access and ensure information is used for authorized purposes.

### Policy: Access

- Only Authorized Users shall access information via the MiHIN.
- Authorized Users will access information via the MiHIN in accordance with all applicable policies, state laws, and federal laws.
- When accessing information, Authorized Users will limit their access to the minimum necessary standard.
- Authorized Users shall be authenticated in accordance with the provisions of the Authentication Policy.
- Passwords shall meet the password strength requirements set forth in NIST SP 800-63 (e.g., the probability of success of an online password guessing attack shall not exceed 1 in 16,384 over the life of the password).
- Group or temporary user names are prohibited.
- Authorized Users shall be required to change their passwords at least every 90 calendar days and shall be prohibited from reusing passwords.
- 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.
- Each authorized user must be identified with a unique user name and password with which to access patient information via the HIE then MiHIN
  - • An authorized user's account will be disabled/blocked after a designated number of consecutive failed attempts to access patient information and will remain blocked until the authorized user can provide appropriate identification/authentication and an administrator releases the account.
  - • HIEs shall ensure that there is an automatic logout after a specified period of inactivity by the user
  - • Each authorized user must receive training from the HIE in order to understand and comply with the policies and procedures for access to patient information
  - • Policy and Procedures must be developed to terminate an authorized user's access promptly due to employment termination/change or other defined situations.
  - • Sanctions must be established to redress policy or procedural violations.

## MiHIN Authorization Policy

The MiHIN will develop and implement minimum policies for Community HIEs to adopt in order to connect to the MiHIN Backbone.

### Policy: Authorization

- Community HIEs shall establish and implement policies and procedures that:
  - Establish categories of Authorized Users;
  - Define the purposes for which Authorized Users in those categories may access Protected Health Information (PHI) via the MIHIN
  - Define the types of PHI that Authorized Users within such categories 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
- At a minimum, Community HIEs shall utilize the following role-based access standards to establish appropriate categories of Authorized Users and to define the purposes for which access may be granted and the types of information that may be accessed:
  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
- Community HIEs shall require Participants to designate the individuals within their organizations who will be authorized to access information via the MIHIN and to assign those individuals to the appropriate categories as listed above.

## **MiHIN Authentication Policy**

The MiHIN will develop and implement minimum policies for Community HIEs to adopt in order to connect to the MiHIN Backbone.

### Policy: Authentication

- Community HIEs must authenticate, or must require their Participants to authenticate, each Authorized User's identity prior to providing such Authorized User with access to Protected Health Information (PHI) via the MiHIN
- All Participants shall implement and enforce a user authentication mechanism.
- Each Authorized User seeking access to electronic PHI transmitted or stored by the MiHIN shall utilize a user authentication mechanism to access the MiHIN.
- The authentication mechanism will be composed of a unique user identification and a token.
- The unique user identification will be username.
- The following tokens may be used to provide user authentication:
  - Passwords;
  - Smart cards;
  - Digital certificates; or
  - Other means approved by the MiHIN
- Authorized Users who have access to electronic PHI via the MiHIN will be required to receive training on the authentication process and mechanisms required for their job function.
- Authorized Users will not share or disclose to others their user authentication information.