



Privacy and Security Sub Work Group Agenda

Meeting Date:	Thursday, January 28, 2010	Facilitator:	Kelly Coyle
Place:	Web-ex	Web-ex Information:	https://premconf.webex.com/premconf/j.php?ED=102879087&UID=0 password: mihin-ps2
Time:	1:30 – 3:30 PM	Teleconference #:	1-888-3948197 passcode 869479

Topic 1:	<p>Housekeeping and Logistics</p> <p>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></p> <p>Approval of meeting minutes Review of Meeting Schedule Review of Meeting Structure Work Zone Review</p>
Topic 2:	<p>Individual Consent</p> <p>State-wide approach for Individual Consent Policy Discussion</p>
Topic 3:	<p>Next Meeting Reminder Tuesday, February 2nd 9-11 am</p>



Agenda and Meeting Minutes

Title / Purpose:	MiHIN Privacy and Security Workgroup Meeting		
Meeting Date:	Jan 7, 2010	Facilitator:	Kelly Coyle
Place:	Kellogg Conference Center	Time:	9:00 A M – 12:00 noon
		Conf Call #:	1-888-394-8197 Passcode: 869479

Attendees:

- Chandra Morse
- Chuck Dougherty
- Cynthia Edwards
- Darrell Dontje
- Denise Chrysler
- Donald Carne
- Gary Lacher
- George Boresma
- George Goble
- Guy Hembroff
- Helen Hill
- Jeff Bontsas
- John Hazewinkel
- Joseph Saul
- Kim Roberts
- Kurt Riegel
- Laura Rappleye
- Linda Young
- Mark LaCross
- Melissa Markey
- Mick Talley
- Mike Tarn
- Moira Davenport-Ash
- Nancy Walker
- Patrick Klima
- Paul Muneio
- Rachel Nosowsky
- Rob Moerland
- Scott Miller
- Stewart Tan
- Teresa Mulford
- Tosca Habel
- Troy Lane
- Vicki McPherson
- Violanda Grigorescu

Topic 1:	Introductions and Welcome	15 Min
Contents:	Co-chair, voting process, Work group expectations	
Presenter:	Kelly Coyle	
Topic 2:	Project Review	30 Min
Contents:	MiHIN Project Overview, Workgroups and Relationships, Where Privacy and Security Fits In	
Presenter:	Kelly Coyle, Mike Gagnon	
Topic 3:	Deliverables and Timeline	30 Min
Contents:	<p>Review of sub work group deliverables</p> <ol style="list-style-type: none"> 1. MiHIN Consent package approach, policy/ plan for implementation 2. Policies and Procedures for Authorization, Authentication, Access, Audit, Breach 3. Draft Strategic Plan P/S section 4. Draft Operations Plan- P/S section 5. Develop draft trust agreements 6. Build on and update HISPC project work for Provider Education and Outreach and Harmonization of State Privacy Law 7. Draft Future plans for Harmonization of Intrastate and Interstate state privacy laws 	
Presenter:	Kelly Coyle, Margaret Marchak	
Topic 4:	Initial Discussion on Consent Package	60 Min
Contents:	<ul style="list-style-type: none"> ▪ Recommended consent form, requirements, exceptions and "break the glass" ▪ Public health reporting ▪ De-identified data ▪ Health information with extra protections (HIV AIDS, mental health, substance abuse, etc.) ▪ Minors 	
Presenter:	Margaret Marchak	
Topic 5	Future Meeting Schedule and Public Comment Period	15 Min

DISCUSSION	Topic 1: Introductions and Welcome	
<p>Kelly discussed the Rules of Engagement, the voting process and what it means to be a voting member. Voting and non-voting members will have access to posted documents. Voting members weigh in on what needs to be done and will have more assignments than non-voting members. Voting members will have more input but non-voting can also participate in all meetings and are also able to speak. Voting and non-voting members can also email questions and comments to the facilitators.</p> <p>This WG will work closely with the Technical WG and Mike Gagnon will provide detail where needed when it comes to technology issues. Once the voting members have been established, we will create a schedule for WG meetings and a timeline for the work that needs to be done. The strategic plan is to be completed by March so there is much work to do.</p> <p>All MiHIN WG materials will be posted on the MiHIN website (www.michigan.gov/mihin) as well as to WorkZone.</p>		
ACTION ITEMS	PERSON RESPONSIBLE	DEADLINE



Request to add Mark Lacross to voting ballots and replace Robert Moerland with Chuck Dougherty.	Sharon McLearn	01-08-10
-------------------------------------------------------------------------------------------------	----------------	----------

DISCUSSION	Topic 2: Project Review
------------	--------------------------------

Mike Gagnon presented a broad description of the conceptual architecture and how the P&S WG should be thinking about policies and procedures going forward. Communication regarding P&S policies for consent, breach notifications, auditing, etc will go back and forth between the two WGs, recognizing that these policies have technical solutions.

The architecture for the MiHIN Backbone is designed following a model of NHIN and that means we are designing MiHIN as a Service Oriented Architecture (SOA) with a 4 tier protocol stack that is fairly rigid in terms of standardization. There will be two main functions of the backbone: Master Patient Index in order to do Subject Discovery (patient inquiry) and Query for Documents where a document is an episode of care like a discharge summary or a package of lab results – not an individual item. The community HIE will do data aggregation – the backbone will share that data among participating HIEs. The backbone will interconnect providers via Community HIEs, to provide shared clinical and administrative services, and will provide connectivity to the NHIN for sharing data with other states and the Federal government. The State of PA has expressed interest in doing a pilot with Michigan to test their NHIN gateway to external sources.

Security is a big part of the conceptual architecture design the Technical WG will be working on very soon. Vendor presentations will help us by providing valuable information. Authenticating users could be role-based and this could make the job of security more manageable. There are other options but it is probable that we will use a role-based security model. Could have the local HIE authenticate the users and then the MiHIN backbone would trust that authentication.

Mike talked through a description of the Conceptual Architecture diagram. There will be a service registry – identifies to external sources what services are available via the MiHIN. The PHR system shown at the top will be private, ie, not sponsored by the state. The backbone will connect to the State of Michigan systems for vital records, immunizations, disease surveillance, etc. If a citizen from Michigan wants to query and retrieve their records and immunizations, we may enable that capability in the future.

Down lower is a symbol that represents a service. Anyone can connect and invoke these services. Public service registry then knows who that is and what standards are out there to support that service.

The Technical WG would like to keep the backbone very dependent on HITSP standards. If the community HIEs have non-standard information exchange at a lower level using local protocols that's OK as long as they meet the structured standards to connect to the backbone. This is an overall principal with the conceptual architecture. It means the MiHIN backbone will be relatively complex to connect with.

On far upper left of the diagram, the reference labs and pharmacies can connect in. We are not looking to have the MiHIN replace existing applications but those applications would need to buy into the structured concept. And Payers are on the diagram at the top. Payers are not at the community HIE level because Payers serve a different function than community HIEs.

Private HIEs and/or affinity groups can connect directly or through a community HIE. Only one connection is needed for information exchange throughout the MiHIN. There is no need to connect to any other community HIE or for any other private connection. It's drawn this way because we only envision 20-25 connections to the backbone. As in a typical network concept lots of traffic is kept local.

Questions from Harvey O. from my1HIE - Security risk assessment as a deliverable – is it an issue and for who? The fact that we should be doing them is a policy decision for P&S SWG. We need to recommend that risk assessment should be done at **all** levels right down to the individual providers. This is an example of how the P&S WG will make recommendations that ripple all the way through the MiHIN effort.

Question was asked about what group will produce the interconnecting security agreement – both the Technical and the P&S WG will do and will negotiate with those connecting to the backbone.

ACTION ITEMS	PERSON RESPONSIBLE	DEADLINE
--------------	--------------------	----------

None.		
-------	--	--

DISCUSSION	Topic 3: Deliverables and Timeline
------------	-------------------------------------------

Margaret thanked the participants and recognized the talent here today.

The P&S WG will be developing a consent package approach as well as trust agreements such as data use and data sharing, and policies and procedures for authentication, access, audit, authorization and breach.

WG will have to consider interstate and intra-state exchanges of health information. (State of PA security laws will be different than MI, for example.) With nine medical trading areas (MTA), hopefully we will develop policies that will be adopted uniformly and consistently across the state. We will be doing this work in order to draft the P&S section for the State's strategic plan and operational plan.

This will be a transparent and open process. We will leverage prior legal workgroup efforts, HISPC work, and what other states have done and documented. We have many resource materials, including the 700 pages recently made public by the Government so there will be lots of reading.

Kelly briefly described the Outreach HISPC project work for provider education and harmonization for state privacy laws that the WG will be expanding on..

ACTION ITEMS	PERSON RESPONSIBLE	DEADLINE
None,		
DISCUSSION	Topic 4: Initial Discussion on Consent Package	

Kelly discussed the MICR Approach for consent and invited the group to discuss the topic.

How will participants decide how they are going to share information – opt-in or opt-out? Under the prior determination of informed opt-out which was approved by the HIT Commission, all data would be included in the HIE in electronic format. If a person chose to opt-out, the data would not be available unless there was an emergency and then “break the glass” would prevail. This WG will need to decide what informed opt out means – if you opt out, will demographic data be available but not PHI? Does it mean certain fields or types of data will be protected and not available? The special categories of information such as HIV/AIDS, substance abuse, mental health, genetic information, etc. will have to be flagged. Can we break the glass on that? We'll have to address what is technically feasible and what is valid under current Michigan law. P&S needs to work through this scenario with the Technical WG.

WorkZone has the prior document and the form for Informed Opt-out. It is built on the MICR model. There are several other consent forms and documents as well. MiHIN will want to make sure a consumer knows *what* they are opting into/out of so there will need to be an education component.

Several comments for possible future discussion included:

- How to keep an eye on minimum necessary. Margaret indicated this doesn't apply for treatment which is the primary purpose of HIE.
- How to deal with VIP patients and what about liability if information is disclosed not by the treating entity but someone else in the HIE.
- Use of aliases is a big issue for authentication.
- Opportunity for real time auditing? Sarbanes-Oxley could be programmed.
- In future the Backbone might store data and initially it would be de-identified – need to think about this.
- Who is responsible for correction of data? The source should be – not the backbone. Need to determine where people will go for corrections.
- Patient identity wrong – question liability for treatment based on incorrect info received from another source. This goes with being able to uniquely identify patients before exchanging the data.
- Data integrity – need to establish a mechanism for reporting data that might not be accurate. The backbone may cleanse MPI data – won't do anything with clinical data.

Kelly pointed out that we'll look at what is done currently – current protection laws will apply, just because information is now electronic, that does not wipe out current law. Also need to keep in mind the standard of care is community based.

Harvey O commented that we must protect consumers against employer and insurance decisions being made based on medical records. Who can legitimately request those records? Could there be a specially protected class of information, from a moral perspective for example. Margaret responded that employers likely will not have any access to the HIE data.

P&S will reach out to ACLU or American Cancer Society for consumer representation on the WG.

Margaret asked if criminal prosecution is enough of a threat to limit unauthorized access?

Chuck Dougherty noted the WG should remember we are at the backbone level, not application level. Mike Gagnon agreed and said PHI on the data warehouse would be de-identified information.

Mike pointed out that consent will need to be done at the provider level. It will be implemented in a way in the network to identify that consent was obtained. Minimum data requirements and rules need to be developed. The system will have to generate a series of messages and will also have to identify that the person requesting is authorized. Must also look at age of consent, especially for interstate exchanges.

Linda McCardel mentioned the HISPC work that was done on age of consent across all states by Joy Pritts, George Washington University. Other HISPC work will be helpful in looking at a number of the privacy and security issues. Melissa Markey noted that harmonization across states will be complex for consent related issues.

Margaret suggested that our scope might be more limited than we first envisioned. For example, P&S could be focusing on the information flowing *across* the network, (the backbone) and not on getting the information onto a system in the first place.

In relation to how the Technical and P&S WG will interact, Mike will develop questions for us that need to be addressed in order to understand how the architecture can deal with the issues. In the case of Public Health reporting the backbone may be able to take burden off providers for individual reporting. This will depend on where data is stored – at the HIE level or the backbone; where data is stored has some “meaningful use” implications as far as reporting goes. We also need to have a full discussion on data ownership, especially if on edge servers. As HIEs mature, it’s easier to get to one data storage rather than have edge servers all over. This is more efficient and allows effective use of the data. The NHIN data use agreement called the DURSA can be useful here.

Chuck Dougherty brought up data that is embedded in another data system and agreements on rerelease of that data – if it’s embedded is it a transfer of ownership? This brought up 42 CFR Part 2 and the prohibition of re-disclosing substance abuse data. This needs federal guidance. We’ll look back at the 2007 recommendations to the HIT Commission as the Legal Workgroup met with SAMHSA at that time. We can look to what other HIEs are doing in this area as well.

Moira Davenport-Ash was concerned about compliance with the HIPAA minimum necessary requirements.

Margaret stated that for medical treatment, minimum necessary does not apply.

Mike suggested that we think about every piece of data being tagged with the source. Could it be an NPI? Mike is thinking about identifying the organization or entity to track the data through the network, not the individual providers that might have created the data. This issue will have to be addressed.

In closing, Kelly reiterated that we have to consider the special protections for sensitive data. The WG will also have to address breach policies and procedures – HITECH was fairly prescriptive but still need to look at enforcement overall. Some answers will have to come from Governance – such as will there be a Privacy Officer for MIHIN? – before P&S can address how to move forward.

ACTION ITEMS	PERSON RESPONSIBLE	DEADLINE
None.		
DISCUSSION	Topic 5: Public Comment and Future Meeting Schedule	
Future schedule would be available as the workgroup and voting members get established.		



MiHIN Privacy & Security Sub Workgroup

Thursday January 28, 2010

1:30-3:30





Privacy and Security Sub Work Group Agenda

Agenda

Welcome

Roll Call of Voting Members

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

Approval of meeting minutes

Review of Meeting Schedule

Review of Meeting Structure

Work Zone Review

**Patient Consent- Discussion of MiHIN Patient Consent Directives
Options**



Voting Members

1. Jeff Bontsas
St John Health System
2. Moira Davenport Ash
CEI Community Mental Health Authority
3. Melissa Markey
Hall Render
4. Denise Chrysler
MDCH
5. John Hazewinkel
Michigan State University
6. Mike Tarn
Western Michigan University
7. Chuck Dougherty
CEI Community Mental Health
8. Glen Lutz
Ascension Health
9. George Goeble
Trinity Health
10. Nancy Walker
Michigan Health Information Management Association
11. Shelli Weisberg
ACLU of Michigan
12. Darrell Dontje
Michigan Department of Information Technology



Meeting Schedule

- Thursday January 28 1:30 to 3:30
- Tuesday February 2 9-11am
- Tuesday February 9 9-11am
- Tuesday February 23 9-11am
- Tuesday March 9 9-11am
- Tuesday March 16 9-11am
- Tuesday March 23 9-11am
- Tuesday March 30 9-11am
- Tuesday April 6 9-11am (*tentative*)



Privacy & Security Meeting Structure

Discussions are open to all members of the work group throughout the meeting- we welcome and encourage everyone's participation

Designated discussion points will occur throughout the meeting- we ask that unless you have strong, relevant concerns you wait until we reach those designated discussion point times to discuss the topic

Privacy and Security team members' expertise and participation are essential to the success of this Sub Work Group. We expect all of our members to participate, read documents and be prepared for the meetings. Your input is critical to our success

We welcome comments anytime regarding this workgroup via email to Kcoyle@mphi.org for suggestions, concerns, questions, etc. You are also free to call me anytime at 517.324.6042 .

When a vote is called, (after discussion) the following process will be followed:

- Voting Work Group Members will be asked for their vote in regards to the particular item
- A quorum (7) of the total number of Voting Work Group Members (12) must vote on an issue or item in order for it to be approved.
- A majority vote of the quorum rules
- When possible, items that require a vote will be clearly noted on the agenda.



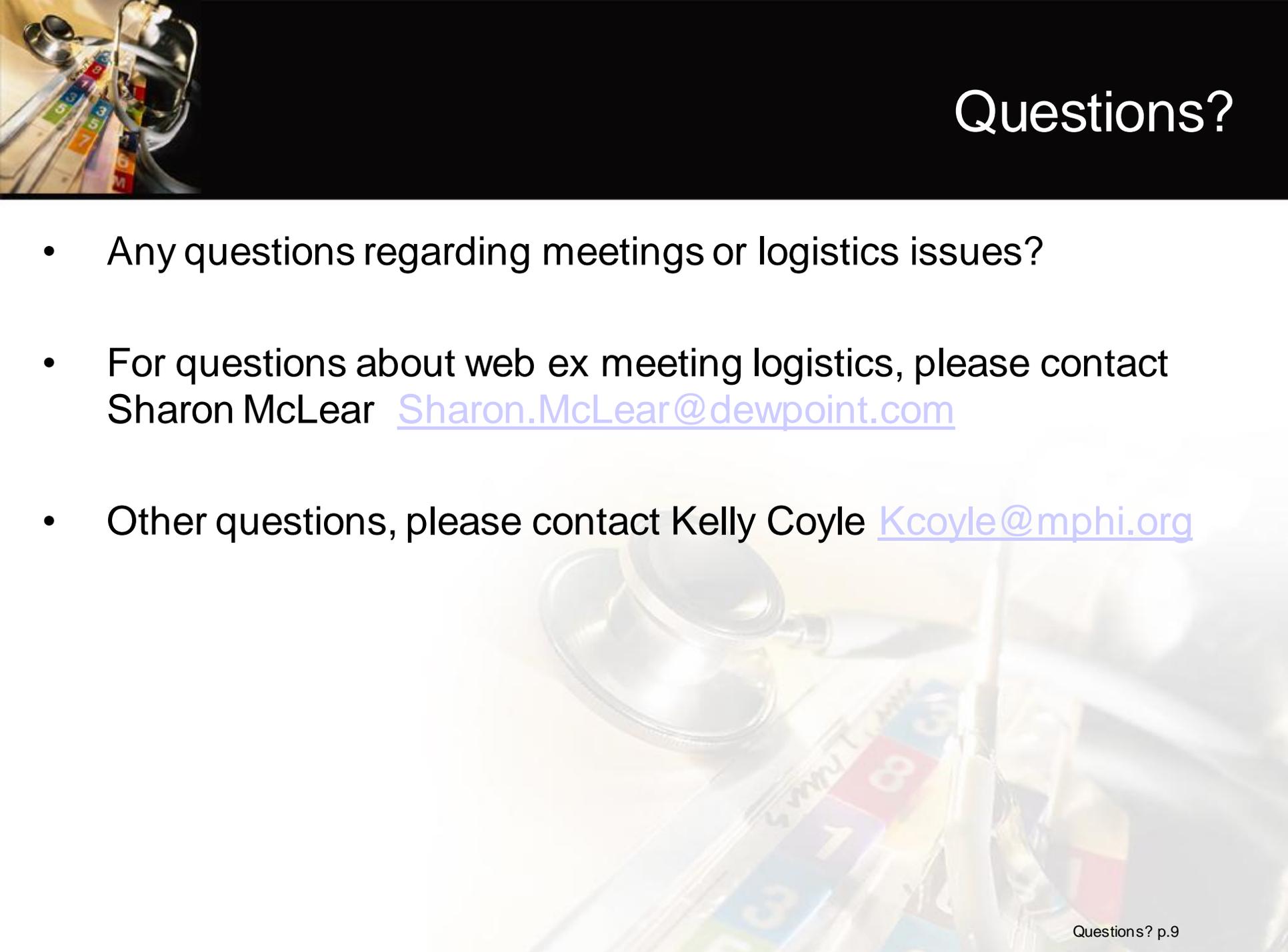
Work Zone

- MiHIN Proposal WorkZone:
<https://dewpoint.sharedwork.com/wz/template/Login.vm?1259090772965>
- MIHIN Privacy and Security Subgroup is our workspace
- Tabs are on the left
 - Reference Materials tab contains background documents that may be helpful
 - Work in Progress is where you'll find Meeting Materials
 - We will post all meeting materials in this area
 - Labeled by date of meeting
 - All meeting materials along with meeting reminders will be emailed to all work group members



Work Zone

- Type in your email address and password
(typically your last name with no capital letters)
- Select your workspace: *Privacy and Security*
(if you have access to more than one)
- Click on the Work-in-Process folder
- You will be able to:
 - access documents
 - email a link to the document to other WZ users
 - add a comment
- For Help
 - help@workzone.com
 - Call 610-275-9861

A stethoscope is positioned in the top left corner of the slide. The background features a blurred image of a desk with a calendar and a pen. The calendar has colorful tabs with numbers and text, including '5 min', '10 min', and '15 min'.

Questions?

- Any questions regarding meetings or logistics issues?
- For questions about web ex meeting logistics, please contact Sharon McLear Sharon.McLear@dewpoint.com
- Other questions, please contact Kelly Coyle Kcoyle@mphi.org

Our first deliverable(s):

- Select the recommended, state-wide approach for Individual Consent for participation in a Community HIE (*the capture and management of consent directives that consumers provide*)
- Draft a policy that meets the minimum technology requirements for the MIHIN, all state and federal legal requirements and provides reasonable guidance for the Community HIEs to follow
- Develop a draft of the elements that may be included in a consent form(s)
- Develop implementation process for the approach

1. Meet legal requirements
2. After meeting legal requirements, then as a policy decision: how do we balance interests to best achieve goals?

Maximize public support & patient trust
a/k/a maximize patient choice and control

HIE Goals

Health Care:

1. Quality
2. Safety
3. Cost savings
4. Efficiency

Maximize ease of data flow a/k/a minimize obstacles to data sharing





Assumptions

- Technology can accommodate any recommendation we draft
- The MiHIN will eventually connect with the NHIN
- All health information will eventually be exchanged electronically
- Community HIEs will manage most operations
- 3%-5% decide to not participate regardless of Opt in or Opt out methodology



General Consent Option Issues

- Duration of consent
- Public health reporting- will the Community HIE (CHIE) be allowed to disclose this data if CHIE participant is currently permitted to disclose?
- Breaking the Glass- will this be allowed if the individual's data is stored regardless of their consent choice? If so under what conditions?
- Converting data- will conversion of paper data to electronic form be included if the individual's information is in the HIE?
- De-identified data- will consent be needed for access/disclosure of de-identified data? IRB approved research? Public Health? Evaluation and quality improvement? Marketing?
- Minors- what's the age? Emancipated minors? Title 10



Consent Options

- **No Consent** *individual's data will be exchanged and included in the HIE without any options offered*-this choice will result in the most information being available to the physician, thus a better quality of care. However, this option may result in less data being available because patients choose not to seek care or less accurate information being available because patients provide incorrect information.
- **Opt In** *individuals have to consent before their information is included in the HIE* this choice will result in less information being available because patients will need to take an action to be included in the system.
- **Opt In with Restrictions** *individuals have to consent before their information is included in the HIE, but can pick and choose what health information to exclude* (then we would have to decide on what would be allowed to be excluded and how) this choice will result in the least information being available to the physician.



Consent Options

- **Opt Out** *individual's data would automatically be included in the HIE, unless they chose not to participate-* this choice will result in more information being available because all patient information will be in the system except for those patients choosing to opt out
- **Opt Out with Exceptions** *individual's data would automatically be in the HIE, but can pick and choose what health information to restrict from being exchanged* this choice will result in some information being available because patient information will be in the system except for those patients choosing to opt out and the information patients choose exceptions
- **Informed Opt Out** *individual's data would automatically be included in the HIE, unless they chose not to participate- but would be well informed (including language in the participants NPP) through outreach and education on the risks and benefits of participation*



Informed Opt Out

Informed Opt Out- ensuring that individuals have a clear understanding about HIE and are educated about the risks and benefits of opting out.

- Previous MIHIN legal work group recommended consent be addressed by the HIT Commission
- A stakeholder group was convened and approved Informed Opt Out for MiHIN participation
- Based on the already successful MCIR model
- Approved unanimously by HIT Commission



Informed Opt Out

Informed Opt Out

- All patient data will be collected and stored at the community HIE level but not all data will be accessible, unless an exception applies (such as ‘break the glass’)
- Specially protected health information will not be exchanged initially in any manner that is contrary to current laws or standards
- Opting Out applies to all levels of the HIE as well as the backbone and sharing with other HIEs.

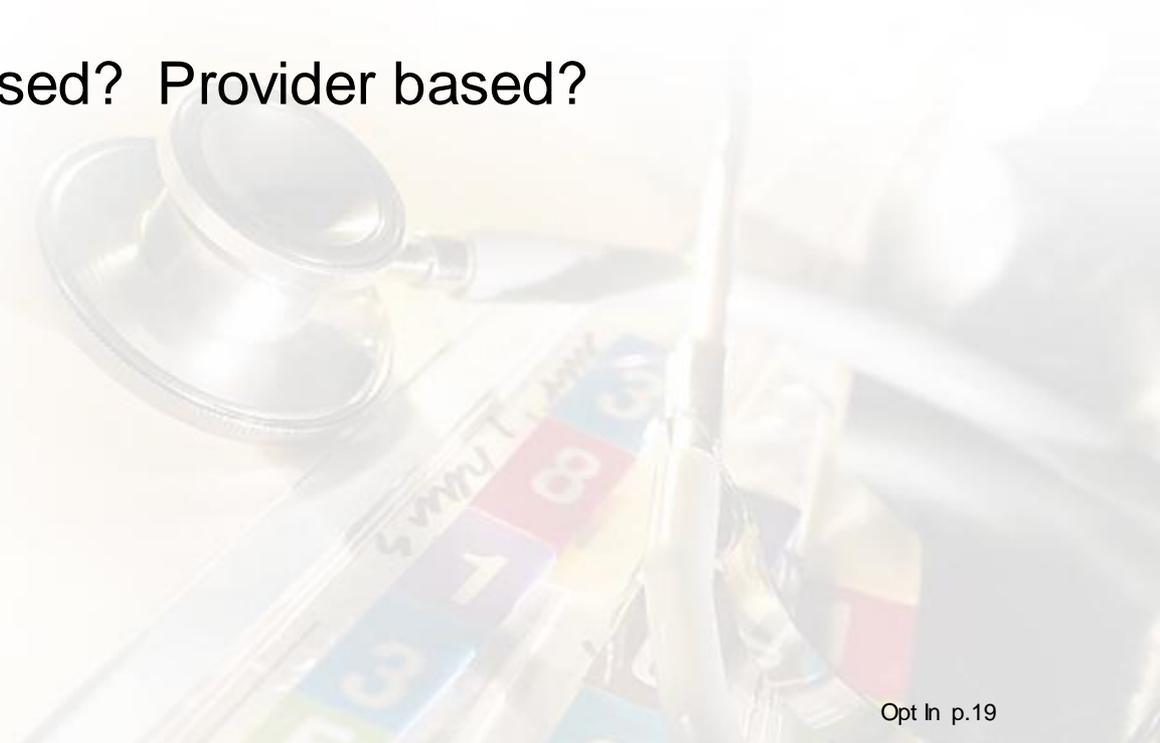


No Consent

No Consent: Under this option, patient's records are automatically placed into the health information exchange (HIE) system, regardless of patient preferences. This alternative assumes that all records of patients of participating entities will be available to the system.

- HIPAA allows for the disclosure of patient health information for treatment, payment and operations without patient consent
- Michigan law requires additional consent for specially protected health information

Opt In: Patient's Health information is not automatically placed into the HIE system, and exchange of health information is not allowed without the patient's prior permission

- Is consent event based? Provider based?
- 



Opt In with Restrictions

Opt In with Restrictions: Patients' health information is not automatically placed into the HIE system, and exchange of health information is not allowed without the patient's prior permission.

This option also allows patients to restrict:

- To whom health information may be disclosed
- The purpose of the disclosure, and/or
- What specific health information may be disclosed

Opt Out: Patient's health information is automatically placed into the HIE system and exchange is allowed for sharing health information without the patient's prior permission. The patient's information remains in the system and is available for electronic exchange unless and until the patient chooses to opt-out of participation.

- Exceptions
 - “Break the glass”
 - Other



Opt Out with Exceptions

Opt Out with Exceptions: Patient's health information is automatically placed into the HIE system and exchange is allowed for sharing of health information without the patient's prior permission. The patient's information remains available for electronic exchange until the patient chooses to opt-out of participation. Patients may specify:

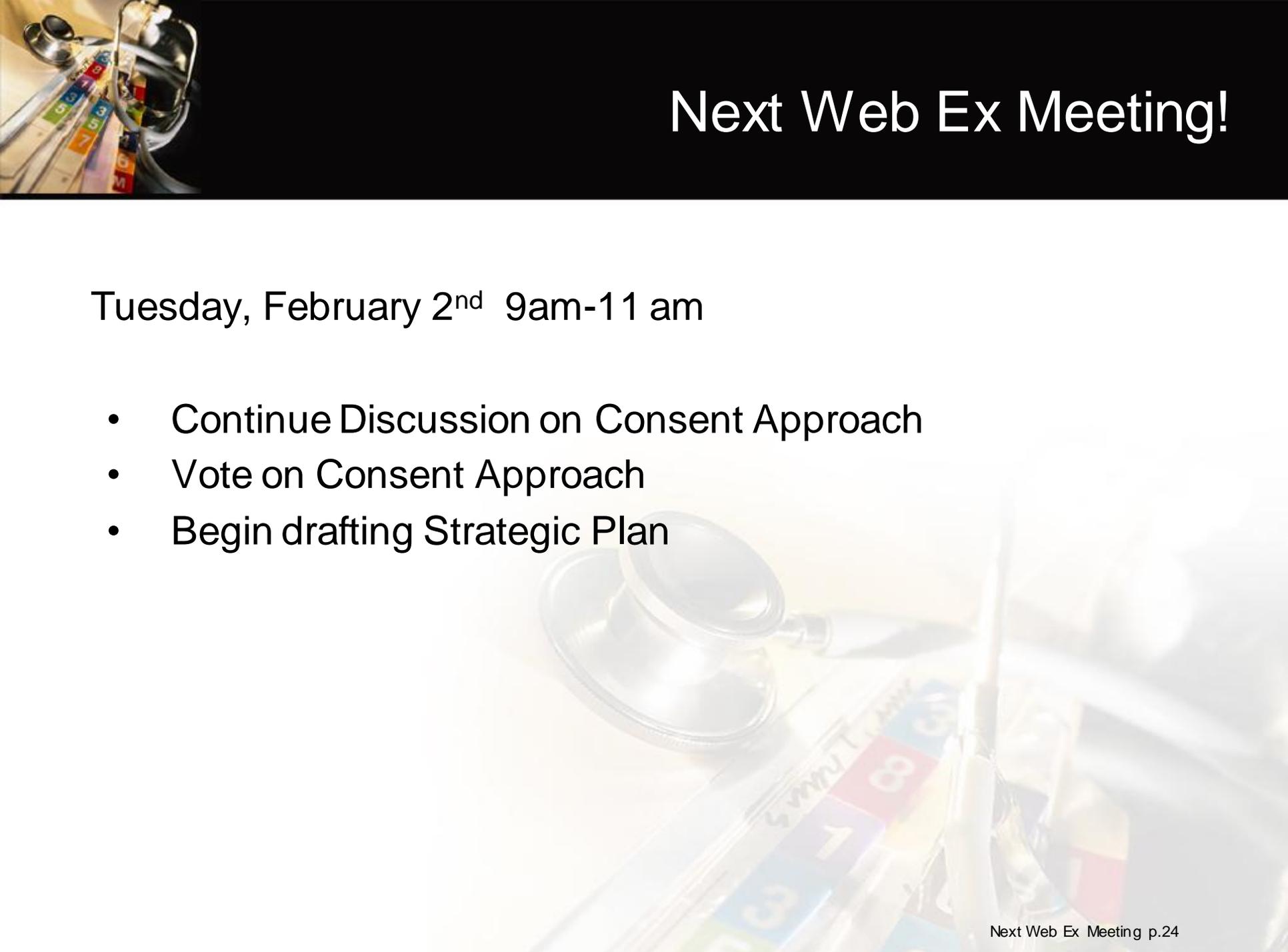
- To whom health information may not be disclosed
- For what purposes health information may not be disclosed, and/or
- What specific health information may not be disclosed
- Exceptions
 - “Break the glass”
 - Other



Questions to Consider

- Is it meaningful?
- Is it administratively burdensome?
- Does it meet legal mandates?
- Is it appropriate from a risk management perspective?
- Is it feasible to implement?
- Does it earn the public's trust
- Does it meet consumer expectations?

DISCUSSION

A stethoscope and a pen are resting on a desk. In the background, a calendar is visible with various dates and colors. The overall scene suggests a professional or medical setting.

Next Web Ex Meeting!

Tuesday, February 2nd 9am-11 am

- Continue Discussion on Consent Approach
- Vote on Consent Approach
- Begin drafting Strategic Plan