



Privacy and Security Sub Work Group Agenda

Meeting Date:	Tuesday Feb 9 2010	Facilitator:	Kelly Coyle
Place:	Web-ex	Web-ex Information:	https://premconf.webex.com/premconf/j.php?ED=102879182&UID=73752177 password: mihin-ps4
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:	Consent- Review Framework Document
Topic 2:	Strategic Plan Discussion Continue Discussion and Review Vote to Approve Strategic Plan Draft



Privacy and Security Third WG Meeting Meeting Minutes

Meeting Date:	Tuesday, February 2, 2010	Facilitator:	Kelly Coyle
Place:	Web-ex	Web-ex Information:	https://premconf.webex.com/premconf/j.php?ED=102879137&UID=73752112 Password: mihin-ps3
Time:	9:00 – 11:00 AM	Teleconference #:	1-888-394-8197 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
Topic 2:	Individual Consent Wrap Up Discussion Vote on Consent Approach
Topic 3:	Strategic Plan Overview Privacy and Security State Laws Policies and Procedures Trust Agreements (for example: data use and data sharing) Oversight and Enforcement
Topic 4:	Next Meeting Reminder Tuesday, February 9 th 9-11 am

Co-Chairs: Margaret Marchak, Beth Nagel

Voting Members Invited (**Attended**): **Jeff Bontsas, Denise Chrysler, Moira Davenport-Ash, Darrell Dontje, Chuck Dougherty, George Goble, John Hazewinkel, Glen Lutz, Melissa Markey, Mike Tarn, Nancy Walker, Shelli Weisberg**

Members Invited (**Attended**): **Don Carne, George Dix, Cynthia Edwards, Harlan Goodrich, Violanda Grigorescu, Tosca Habel, Carol Heinicke, Guy Hembroff, Helen Hill, Vik Kheterpal, Patrick Klima, Gary Lacher, Mark LaCross, Troy Lane, Jim Lee, Harry McGee, Vicki Mcpherson, Scott Miller, Robert Moerland, Chandra Morse, Deb Mosher, Teresa Mulford, Paul Muneio, Rachel Nosowsky, Kurt Riegel, Kim Roberts, Joseph Saul, Cindy Seel, Micheal Stines, Jeanne Strickland, Mick Talley, Stewart Tan**

MiHIN PCO/MPHI Invited (**Attended**): David Allen, George Boersma, **Kathy Cornish**, Audra Cumberworth, **Mike Gagnon, Harry Levins, Pat Maltby, Linda McCardel, Sharon McLearn, Amber Murphy, Samer Naser, Laura Rappleye**

Technical Workgroup Members: **Bruce Weigand (Voting)**



DISCUSSION	Topic 1: Housekeeping and Logistics
------------	-------------------------------------

Roll Call of Voting Members: All present

Approval of meeting minutes: Pending changes to be sent following this meeting by a voting member

MOTION: Approve meeting minutes after receipt and update to be sent by voting member

MOTION SECONDED

VOTE: Approved (all present Voting Members)

ACTION ITEMS	PERSON RESPONSIBLE	DEADLINE
Update and finalize previous meeting minutes	Sharon McLear	

DISCUSSION	Topic 2: Individual Consent and Vote on Consent Approach
------------	--

- Do we want to break consent into pieces where there are separate consents for information flowing in and information flowing out? Or is the info flow in by default and the consent is for letting the information flow out? Comments from the discussion are listed below.

Discussion/Comments:

- From a security perspective, the security and privacy risk is greater with electronic information, as opposed to paper records.
- With the MiHIN the risk is also that the data is going to be in two places; edge server(s) and the HIE. Another way to consider consent is from two levels: Patient level consent and Provider level consent.
- Another consideration, we could have information flow into the regional HIE without needing a consent (i.e., by default) and that person opts out of having that information flow out, then if there is a breach at the regional HIE, it is a problem. This is a risk.
- It would be wise to avoid requiring authorization for hospitals to get to the information.
- The information is 'aggregated' information stored in edge servers. Maybe the consent is: consent to be part of the aggregated information.
- The 1 to 1 information transfer could happen without consent because this is the normal business practice of pushing information out. A physician uses discretion about what another physician requires. Other states view this as an implied consent; this is why it is the use of aggregated information that requires consent (Mike G).
- Patient Education - when you think about a patient being educated about opt-out, the simpler it is to explain and understand; the better. Will separating the consents into two categories make it simple for educating the patient?
- Scenario to consider: think of one consent 'episode', when the patient is seen initially and agreeing to an information flow in on a going-forward basis (history will *not* go into the MiHIN). This is a benefit to the providers because they will now be able to look up instead of having to request information. Or the patient can opt-out completely. This one consent 'episode' could be one conversation with the patient, even though there are two levels of consent being agreed to. It would be phrased in a way that the patient is normally used to giving consent. Another way to think of this is visiting the doctor for the first time and doing paperwork, one consent allows the doctor to put a document on the network and the other consent allows it to be retrieved.

Question: "What are other states doing?"

Answer: NY is doing one episode of consent and giving one form of consent only and also allowing opt-out completely as an option (Mike G).

- o Comment: Is this too much burden on the providers? It is a one-time consent for the data to flow in and provider by provider for data to flow out.
- In current notice of privacy practices, much of the information a patient would need to be informed of is already in the notice.
- Audit Comments;
 - o Capabilities will be pervasive with the results viewable by the patient.
 - o Audit function needs to be careful about how it reports queries into a patient's information and who is performing those queries. It could lead to misunderstanding and many questions by the patient to the provider office if not handled appropriately.

- Having data available makes for better health care in general:

While there could always be a breach, much of the information being discussed is already being shared. Informed opt-out falls well within the range of what is currently cited in the notice of privacy practices.

Option to consider:

Informed opt-out and information flowing in by default with protection for special information that still needs to be available on Break the Glass. And excluding 1-to-1 exchange as a physician responding to another physician's request allows providers the ability to transfer everything they need.

- Another way to view this is to consider Health information exchange acting as a business associate of the physician.
- Student Pole of (32) Senior College students (Mike Tarn) indicates that while the students would like to be informed about the process, and the system, they assume they can trust the technology. Their preference was for Informed Opt-Out.

Comment: It's possible we are over-complicating this, would a better/different framework assist in the discussion?

Question: In light of the discussions, what is the recommendation for proceeding?

Suggestion: Workgroup needs to flesh out the other pieces of the work they have to do and there is about 2 ½ weeks in the schedule for us to focus on that. While the initial thought was to tackle consent because a lot of work had been done previously, items in the Strategic Plan could help us do the consent policies...

Question: What data should be restricted?

Question: How does Capital Area RHIO handle this now?

Answer (captured via WebEx chat): Capital Area RHIO is following the informed opt-out policy because they understood that it was the policy of MiHIN at the time. The CARHIO Privacy & Security task force discussed other options but left this alone for now..

MOTION (sent via WebEx Chat): add the following considerations for Consent:

1. **No Choice** (flow in and flow out) for prescription info, including 1 to 1 transfer. This information is so crucial to care that safety concerns outweigh all other concerns. Exception for flow out when law requires otherwise.

MOTION SECONDED

MOTION:

2. Retrieve - informed opt-out "with restrictions". Restrictions are not what the patients says, but restrictions are what are either required by law (that requires an affirmative consent) or that we decide as a policy matter needs to be an opt-in because it is so sensitive this is needed for patient trust.

MOTION WITHDRAWN

DISCUSSION:

The group agreed on #1 of - **with the addition of one to one transactions- meaning when a provider exchanges information with another provider but uses the MIHIN as a conduit to share that information- in this case there is no data from this one to one transfer that is stored.**

In regards to #2- the discussion regarding sensitive data needs additional fleshing out- we need to know what each state and federal law says in regards to consent and authorization for access- without knowing these things we won't know which will have to be restricted. It was brought up that we could just say that "all specially protected health information will be exchanged only as permitted by law" until we get to the analysis, which this may have to wait until after this project is completed and could be left for the next phase of the MIHIN.

- Something to keep in mind: a very limited amount of information is going to be exchanged between a limited group- 2 HIEs.
- With consumers option to Opt-out, inclusions will be as much information as possible. Prescriptions and medications would also flow regardless of restrictions.
- Sensitive Information (e.g. prescriptions)
 - o Other sensitive information
 - o Sensitive information protection by law. Legislature has already listed what is sensitive and protected by law
List of sensitive information that continues to surface and that needs more granular discussion:
 - HIV AIDS
 - Mental Health
 - Substance Abuse

- Genetics
- Reproductive Health (no current restrictions (title 10)
- Minors

- NOTE: With respect to sensitive data: the public is sensitive about employers, insurers, spouses, neighbors viewing this information, not clinical users. The workgroup has to focus on CLINCAL use.
 Example: when a neighbor looks up another neighbors' health information, this is miss-use and we have to have specific strong measures for dealing with that.
- Workgroup needs to keep in mind what information will be exchanged in the roll-out of the initial use cases. Some of the detail could be left to work out later.

MOTION:

Eliminate Options 1 and 2 from list of original options regarding how MiHIN will proceed with respect to consent, further consider, discuss and add detail prior to voting on Options 3 and 4

MOTION SECONDED

VOTE: 2 Absent; 1 No; 9 Yes

PARKING LOT:

Patient identifier (Nancy Walker)

Recommendations: Privacy Officer, Security Officer, Audit body, infrastructure around MiHIN (not just a conduit), possibly at the HIE community level

ACTION ITEMS	PERSON RESPONSIBLE	DEADLINE
1. Consent Summary document will be distributed (and posted) for comments (sent to Kelly or posted on WorkZone), including relevant state laws and consent requirements	Kelly Coyle	

DISCUSSION	Topic 3: Strategic Plan Overview
-------------------	----------------------------------

The drafted Strategic Plan will explain how the State plans to implement HIE in Michigan and our group is responsible for addressing the legal and privacy aspects of the plan. We'll need to fill in with the policies and procedures that will cover consent, the 4 As and breach. Once this is completed, we'll address the Operational Plan.

ACTION ITEMS	PERSON RESPONSIBLE	DEADLINE
1. Read Draft Strategic Plan in preparation for discussion at next meeting	Workgroup	Feb 9, 2010

Informed Opt Out

- Decided: All legally allowable data will flow into the HIE

- All data flows out to all providers who are involved in treatment of individual *
 - Consent is obtained provider by provider?
 - Consent is assumed for all treating providers?

- What happens when an individual Opt Out?
 - Does the data stay in the Community HIE, but does not flow out unless there's a "break the glass" situation- or the individual changes their mind?
 - Is the data is purged from the HIE and therefore not available period?

- Questions-
 - What happens to the data in a one-to-one transfer? Is it truly a conduit between the two providers with no storage?
 - What happens to data once it flows to another Community HIE? Is it stored there as well?

- *To address the Exceptions for Specially Protected Health Information:
 - All data that is legally allowed to be exchanged via paper will be allowed to be exchanged via the HIE.
 - If state or federal law requires an additional consent, all providers must obtain that consent in order to access the individual's information from the HIE.

- Questions:
 - Can data be flagged/tagged by document type and/or by type of provider to identify specially protected health information?

Strategic Plan Legal/Policy

Guiding Principles and Requirements

The MiHIN Privacy and Security work group will focus on building consensus within the work group to ensure that the privacy and security protections of health information are balanced with the needs of Michigan stakeholders. In addition, through the production of workgroup deliverables via workgroup meetings and discussions, the work group will provide insight and education to all its members on critical issues related to the privacy and security of health information exchange in Michigan.

The work group will also review applicable state and federal laws and balance them to ensure that policies and procedures are in compliance with those laws in a manner that supports health information exchange while fostering trust and ensuring privacy and security in support of intra and interstate HIE.

Wherever possible, this workgroup will utilize applicable materials produced by approved sources - to avoid "reinventing the wheel".

This work group is a sub work group of the Technical work group and will rely on input from that workgroup in regards to technical specifications and guidelines in drafting policies and procedures.

This outline is based on the required sections of the ONC's Operational and Strategic plan which are the primary deliverables of this project. In addition, the other primary deliverables are the drafting of shovel ready policies and procedures for Michigan's Community HIEs.

1.0 Describe the state's privacy and security framework, (which must consider federal and state laws and regulations and adherence to the privacy principles articulated in the HHS Privacy and Security Framework.)

1.0.1 Privacy Principles (these will likely get put into an appendix- but for now, wanted work group see them up front)

1.1 Address **intrastate** privacy and security issues related to HIE

Overcoming organizational policies and procedures that are more stringent than State and Federal laws

Ensuring compliance with policies and procedures

Hospitals and other providers participating in HIE will need to rely on each other, as well as the exchange system, to ensure records are accurate- to ensure data integrity, and there must be a level of trust between

1.2 Address **interstate** privacy and security issues related to HIE

Over several decades, states have passed laws to protect the privacy of health information. These laws differ from state to state and often narrowly target a particular population, health condition, data collection effort, or specific types of health care organizations. As a result, states have created a patchwork of privacy protections that are not comprehensive or easily understood. Many states also have begun to consider information security related issues and have passed laws, for example, requiring various types of entities to provide notice of security breaches of individually identifiable information.

At the Federal level, there are also a variety of laws related to the privacy and security of health information, including the HIPAA Privacy and Security Rules, the Privacy Act of 1974, the Confidentiality of Alcohol and Drug Abuse Patient Records Regulation (42 CFR Part 2), the Family Educational Rights & Privacy Act (addresses privacy of information held by certain educational institutions), Gramm-Leach-Bliley Financial Services Act (addresses privacy of information held by financial institutions), and Federal Information Security Management Act of 2002 (FISMA).

The Privacy and Security Rules promulgated under HIPAA were the first Federal regulations to broadly address the privacy and security of health information. They establish a baseline of national privacy and security standards for individually identifiable health information held by “covered entities” and a foundation of protection regardless of health condition, type of health program, population, state where the activity occurs, or other situational characteristics.

Although the HIPAA Privacy and Security Rules apply to health information in electronic form, the current landscape of electronic health information exchange poses new issues and involves additional organizations that were not contemplated at the time the rules were drafted.

While the HIPAA privacy and security regulation provides a common standard for maintaining the privacy and security of patient information such standard, as is commonly said, is the “floor and not the ceiling”. State laws which provide patients with privacy and security protections and/or access rights that are greater than HIPAA are not preempted by HIPAA.

At first glance, state laws that provide patients with privacy and security protections and access rights that are greater than HIPAA would seem to be a positive benefit. However, for many practical purposes, the patchwork of medical privacy laws throughout the 50 states has served to create barriers to the appropriate exchange of medical information. Barriers range from the inability to exchange patient information for treatment purposes in a timely manner to inconsistencies in public health reporting and disclosures.

Interoperability Challenges:

- Inconsistent laws addressing the disclosure or re-disclosure of information treatment purposes.
- Inconsistent laws addressing the disclosure of “sensitive” patient information.
- Inconsistent laws addressing the disclosure of public health information (immunization records, communicable diseases, etc..) among states.
- Laws, designed for paper based HIE, which fail to address current modes of transmission and/or storage of electronic data. (Electronic Transmission/Electronic Signatures).
- Lack of uniform consent/authorization forms

1.3 Provide plans to analyze and/or modify state laws- will utilize HISPC Comparative Analysis Matrix review and update

1.3.1

	Citation/ Link	More Stringent than HIPAA for Patient Care?	More Stringent than HIPAA for Population Health?	References to Related State/ Federal Law & Legislative Proposals	Statutory or Regulatory Change Needed?
		Y/N	Y/N		Y/N
Subject Matter					
Privacy Specific Provisions					
Comprehensive general privacy act					
Comprehensive medical privacy act					
Constitutional right to privacy					
Restrictions on use of Social Security number				Freedom of Info. Act	
HIPAA-Based and Other Federally-Based Provisions					
Provisions adopting HIPAA requirements					
Provisions adopting other federally-based provisions				HIPAA (42 CFR Part 2)	
Health Information Provisions					

Health information exchange specific provisions					
Electronic health/ medical record specific provisions				HIPAA (45 CFR 164.302 et seq.)	
Breach of electronic security reporting - general	<input type="checkbox"/> Identity Theft Protection Act (MCL 445.72: Notice of Security Breach; Requirements)			HIPAA (45 CFR 164.302 et seq.) HITECH	
Breach of electronic security reporting - health records	<input type="checkbox"/> Identity Theft Protection Act (MCL 445.72: Notice of Security Breach; Requirements)				
Telehealth/ telemedicine provisions					
Electronic signatures	<input type="checkbox"/> Uniform Electronic Transactions Act (MCL 450.831: Terms and conditions for using electronic signatures and information of business transactions) <input type="checkbox"/> Public Health Code- (MCL 333.17753: Centralized prescription processing, etc.)			Federal E-Sign Law (15 U.S.C. 96)	
Personal health records					
Uniform Electronic Transactions Act	<input type="checkbox"/> Uniform Electronics Transactions Act (MCL 450.832 to 450.846: Electronic signatures and information of business transactions)				
Technical security of electronic systems provisions				HIPAA (45 CFR 164.312)	
Health/Medical Records in General					
Records retention requirements	<input type="checkbox"/> Public Health Code (MCL 333.16213: Retention of Records; MCL 333.20175: Patient records) <input type="checkbox"/> Release of Information for Medical Research and Education (MCL 331.531: Disclosures to peer review entities) <input type="checkbox"/> Michigan Court Rules (MCR 2.314: Release of medical information by subpoena)			HIPAA (42 CFR 482.24, 431.306)	
Patient access	<input type="checkbox"/> Release of Information for Medical Research and Education (MCL 331.531: Disclosures to peer review entities) <input type="checkbox"/> Revised Judicature Act of 1961 (MCL 600.2157: Waiver of physician-patient privilege)			HIPAA (42 CFR 431.306 d)	

Ow nership of medical records	<input type="checkbox"/> Public Health Code (MCL 333.16213: Retention of Records; MCL 333.20175: Patient records; MCL 333.20175a: Agreement w ith another health facility to protect, maintain and provide access to records, etc.)				
Accounting for disclosures					
Specific redisclosure prohibitions					
Redisclosure statement required				HIPAA (42 CFR 2.32)	
Disposition/ destruction of records	<input type="checkbox"/> Public Health Code (MCL 333.20175: Patient records; MCL 333.20175a: Agreement w ith another health facility to protect, maintain and provide access to records, etc.)				
Consent/Authorizations					
Patient consent requirements	<input type="checkbox"/> Mental Health Code (MCL 330.1707: Rights of Minor) <input type="checkbox"/> Public Health Code (MCL 333.5127: Consent by minor for VD or HIV testing; MCL 333.6121: Consent by minor to substance abuse treatment; MCL 333.17015: Informed consent)			HIPAA (42 CFR 431.306 d; 45 CFR 164.510, 164.514)	
Patient authorization requirements				HIPAA (42 CFR 431.306 d)	
Disclosure for emergency situations	<input type="checkbox"/> Public Health Code (MCL 333.17015: Informed consent)			HIPAA (42 CFR 431.306 d; 45 CFR 164.512)	
Minors					
Age of majority	<input type="checkbox"/> Status of Minors and Child Support (MCL 722.4: Emancipation of minor) <input type="checkbox"/> Age of Majority Act of 1971 (MCL 722.52: Adult of legal age, etc.)				
Emancipated minors	<input type="checkbox"/> Status of Minors and Child Support (MCL 722.4e: Rights and responsibilities of emancipated minor; obligation and liability of parents)				

Age consent requirements - mental health	Mental Health Code (MCL 330.1498: Notice to parent of hospital admission of minor; <u>MCL 330.1716</u> : Surgery consent; <u>MCL 330.1707</u> : Rights of minor; <u>MCL 330.1724</u> : Fingerprints, photographs, etc.)				
Age Consent requirements - other conditions	<input type="checkbox"/> Public Health Code (<u>MCL 333.17015</u> : Informed consent for abortion) <input type="checkbox"/> Marriage License (<u>MCL 551.103</u> : Persons capable of contracting marriage; age requirement; etc.)				
Patient Proxies					
Personal Representatives/ Executors	<input type="checkbox"/> Medical Records Access Act (MCL 333.26263: Definitions)				
Guardians	<input type="checkbox"/> Medical Records Access Act (MCL 333.26263: Definitions)				
Health Care Power of Attorney	<input type="checkbox"/> Estates and Protected Individuals Code (<u>MCL 700.5501</u> : Durable Power of Attorney; definition)				
Health Care Power of Attorney - mental health	<input type="checkbox"/> Mental Health Code (<u>MCL 330.1716</u> : Surgery; consent; <u>MCL 330.1433</u> : Assisted outpatient treatment, etc.)				
Health Condition/ Situation Specific Provisions					
Genetic information	<input type="checkbox"/> The Insurance Code of 1956 (<u>MCL 500.3407b</u> : Nondiscrimination based on genetic information) <input type="checkbox"/> Public Health Code (<u>MCL 333.17020</u> : Consent to genetic testing) <input type="checkbox"/> The Nonprofit Health Care Corporation Reform Act (<u>MCL 550.1401</u> : Offering of health care benefits, etc.)			Genetic Information Non-discrimination Act of 2008	
HIV/ AIDS information	<input type="checkbox"/> Public Health Code (<u>MCL 333.5114</u> : Reporting HIV test results; <u>MCL 333.5114a</u> : Partner notification of HIV test results; <u>MCL 333.5119</u> : HIV test for marriage licenses; <u>MCL 333.5123</u> : VD, HIV or Hepatitis B tests for pregnant women; <u>MCL 333.5127</u> : Consent by minor for VD or HIV testing; <u>MCL 333.5129</u> : Communicable disease test results of prostitutes and intravenous drug users; <u>MCL 333.5131</u> : Confidentiality of HIV or AIDS test results; <u>MCL 333.5133</u> : Consent forms for HIV and AIDS testing; <u>MCL 333.16267</u> : Obligation to report positive HIV test results; <u>MCL 791.267</u> : Testing of prisoners for HIV)				

Sexually transmitted disease information					
Hepatitis C information	<input type="checkbox"/> Public health Code (MCL 333.5123: VD, HIV or Hepatitis B tests for pregnant women)				
Adult mental health	<input type="checkbox"/> Public Health Code (MCL 333.6521: Records confidential; disclosure; MCL 333.6111: Records confidential; limitations on disclosure)				
Children's mental health	<input type="checkbox"/> Foster Care and Adoption Services Act (MCL 722.954c: Release of child's medical records, etc.) <input type="checkbox"/> Mental Health Code (MCL 330.1498j: Notification to parent or guardian of hospital admission of minor)				
Communicable disease information	<input type="checkbox"/> Rule 325.173: Reporting of Diseases and Infections <input type="checkbox"/> Rule 325.181: Confidentiality of Reports			42 CFR Part 70	
Alcohol addiction	<input type="checkbox"/> Rule 325.14304: Substance Abuse Treatment Program Patient's Right to Review Records <input type="checkbox"/> Rule 325.14910: Content and Maintenance of Patient Records for Substance Abuse Treatment Programs			42 CFR Part 2	
Drug addiction	<input type="checkbox"/> Rule 325.14304: Substance Abuse Treatment Program Patient's Right to Review Records <input type="checkbox"/> Rule 325.14910: Content and Maintenance of Patient Records for Substance Abuse Treatment Programs			42 CFR Part 2	
Reproductive rights	<input type="checkbox"/> Public Health Code (MCL 333.17015: Informed consent, etc.; MCL 333.2834: Report of fetal death, etc.; MCL 333.9132: Consent of minor to provision of health care, etc.; MCL 333.2835: Abortion reporting)				
Minor wards of the state	<input type="checkbox"/> Probate Code of 1939 (MCL 710.44: Consent to adoption; separate instrument, etc.)				
Adult wards of the state					
Reporting of abortions	<input type="checkbox"/> Public Health Code (MCL 333.2835: Abortion Reporting; MCL 333.2837: Abortion-related deaths or complications; MCL 333.17015: Informed consent)				
Victims (domestic violence, sex assault, etc.)					
Futile Care Provisions					

Other proxies					
Provider Specific Provisions					
Pharmacy records	<input type="checkbox"/> Public Health Code (MCL 333.17752: Prescription or equivalent record; preservation; disclosure; etc.)				
Emergency services (ambulance/ EMT)					
Health profession licensing	<input type="checkbox"/> Public Health Code (MCL 333.16608: Health profession specialty field license, etc.; MCL 333.16196: License or registration of individual inducted or entering into service; continuation; notice; MCL 333.16221: Investigation of licensee, etc.)				
Health profession accreditation	<input type="checkbox"/> Public Health Code (MCL 333.16148: Board; rules establishing standards for education and training; accreditation of training programs; etc.; MCL 333.20155: Facility accreditation and audits)				
Professional counselors	<input type="checkbox"/> Public Health Code (MCL 333.18117: Confidentiality of counselor communications) <input type="checkbox"/> The Revised School Code (MCL 380.1531: Requirements for issuing licenses and certificates and endorsements as qualified counselors etc.)				
Utilization, peer & quality review	<input type="checkbox"/> Public Health Code (MCL 330.1143a: Confidentiality of peer review information for psychiatric facilities; MCL 333.21515: Confidentiality of hospital peer review records)				
Facility-Specific Provisions					
Hospitals	<input type="checkbox"/> Rule 325.1028: Hospital Medical Record Requirements			HIPAA (CFR 42 482.24)	
School-based clinics					
Imaging labs and centers					
Testing and clinical labs	<input type="checkbox"/> Rules 325.1743 and 325.1475: Laboratory Reports			HIPAA (42 CFR 493)	

Assisted living facilities	<input type="checkbox"/> Public Health Code (MCL 333.21743: Confidentiality of clinical records by MDCIS, MDCH and nursing homes; MCL 333.21763: Confidentiality of communications by nursing home residents) <input type="checkbox"/> Mental Health Code (MCL 330.1433: Assisted outpatient treatment, etc.; MCL 330.1469a: Treatment program as alternative to hospitalization; court order) <input type="checkbox"/> Adult Foster Car Facility Licensing Act (MCL 400.712: Keeping and maintaining records and reports; etc.) <input type="checkbox"/> Rule 325.20112: Nursing Homes' Policies for Access to Records <input type="checkbox"/> Rule 400.14316 and Rule 400.15316: Maintenance of Resident Records by Adult Foster Care Group Homes <input type="checkbox"/> Rule 325.1851: Records of Homes for the Aged <input type="checkbox"/> Rule 325.1853: Content of Homes for the Aged Records <input type="checkbox"/> Rule 325.20404: Life-Threatening Accidents or Injuries in Nursing Home				
Drug & alcohol treatment facilities	<input type="checkbox"/> Rule 325.14304: Substance Abuse Treatment Program Patient's Right to Review Records <input type="checkbox"/> Rule 325.14910: Content and Maintenance of Patient Records for Substance Abuse Treatment Programs			HIPAA (42 CFR)	
Rehabilitation facilities					
Home health agencies					
Payers/Insurance Company Provisions					
Health insurance related provisions					
HMO provisions	<input type="checkbox"/> The Nonprofit Health Care Corporation Reform Act (MCL 550.1401(3)(e): Nondisclosure of genetic information; MCL 550.1406: Confidentiality of records; disclosure; etc.; MCL 550.1407: Complaint system; MCL 550.1604: Confidentiality: violation as misdemeanor; penalty) <input type="checkbox"/> Rule 324.6405: HMO Contracts <input type="checkbox"/> Rule 325.6805: HMO Patient Records <input type="checkbox"/> Rule 325.6810: Confidentiality of HMO Clinical Patient Records				

Medicaid/ Medicare related provisions					
Employer Specific Provisions					
EHR					
Provisions related to employers	<input type="checkbox"/> Rule 325.52116 : Employer Retention of Medical Records <input type="checkbox"/> Rule 325.70015 : Employer's Duties as to Medical Records <input type="checkbox"/> Rule 325.70111 : Employer to Maintain Exposure and Exposure-Related medical Records			HIPAA (45 CFR 164.308, 164.314, 164.501, 164.506)	
Preemployment screenings					
Employee assistance programs					
Public Health Reporting					
New born screening	<input type="checkbox"/> Public Health Code (MCL 333.5430 : New born screening quality assurance advisory committee, etc.; MCL 333.5721 : Reporting birth defects) <input type="checkbox"/> The Nonprofit Health Care Corporation Reform Act (MCL 550.1401 : Offering of health care benefits; etc.)				
Vital records (birth/ death certificates)	<input type="checkbox"/> Public Health Code (MCL 333.2821 : Vital records; MCL 333.2833 : Recording death, etc.; MCL 333.2834 : Report of fetal death, etc.; MCL 333.2835 : Abortion reporting; MCL 333.2844a : Release of information to find missing persons; MCL 333.2888 : Inspection and disclosure of vital records) <input type="checkbox"/> Rule 325.3203 : Confidentiality of Vital Records Collected by State Registrar <input type="checkbox"/> Rule 325.3233 : Listing of Marriages, Divorces and Deaths by Registrar <input type="checkbox"/> Rule 325.3234 : Inspection of Vital Records Maintained by Registrar <input type="checkbox"/> Rule 325.3235 : Security of Records Maintained by Registrar				
State Department of Health reporting (reporting certain conditions to state)	<input type="checkbox"/> Public Health Code (MCL 333.16238 : Confidentiality of information, etc.; MCL 333.16243 : Reports, etc.)				
Reports to other state agencies					

Immunization reporting	<input type="checkbox"/> Public Health Code (MCL 333.9206: Certificate of immunization required, etc.)				
Registries					
Information sharing in public emergencies	<input type="checkbox"/> Public Health Code (MCL 333.20191: Infectious agent and emergency treatment)				
State Facilities/Medical Records					
Other state facilities					
Public health clinics					
Correctional facilities (adult)	<input type="checkbox"/> Corrections Code of 1953 (MCL 791.234: Prisoners subject to jurisdiction of parole board, etc.: MCL 791.267: Testing of prisoners for HIV)				
Correctional facilities (minors)					
State hospitals					
State Freedom of Information Act					
Penalties/Remedies					
Statutory right to sue for damages related to health information	<input type="checkbox"/> Public Health Code (MCL 333.21773: Involuntary transfer or discharge of patient; notice; etc.; MCL 333.20201: Policy describing rights and responsibilities of patients or residents; etc.)				
Common law right to sue for damages related to health information					
Criminal provisions - wrongful access					
Administrative penalties for wrongful disclosure					
Litigation Related Provisions					
Medical record subpoenas	<input type="checkbox"/> Public Health Code (MCL 333.20175: Maintaining record for each patient; confidentiality; w ronfully altering or destroying records, etc.; MCL 333.7333a: Electronic monitoring system; MCL 333.16221: Investigation of licensee, registrant, or applicant for licensure or registration, etc.) <input type="checkbox"/> Mental Health Code (MCL 330.1748: Confidentiality of Mental Health Records) <input type="checkbox"/> MCR 2.314: Release of medical information by subpoena <input type="checkbox"/> MCR 2.506: Compliance w ith Subpoena by Hospitals				
Patient/ provider privilege					

Workers comp disclosures	<input type="checkbox"/> Workers Disability Compensation Act (<u>MCL 418.230</u> : Confidential records; power of court to subpoena records not limited)				
Law Enforcement					
DUI test results	<input type="checkbox"/> Michigan Vehicle Code (<u>MCL 257.625a</u> : Arrest without warrant; availability of test results, etc.)				
Abuse & neglect	<input type="checkbox"/> Mental Health Code (MCL 330.1723: Obligation of mental health professional to report abuse or neglect; MCL 330.1748a: Use of mental health records as evidence of abuse or neglect) <input type="checkbox"/> Public Health Code (<u>MCL 333.2640</u> : Provision of medical records for child abuse or neglect; <u>MCL 333.16281</u> : Disclosure of Child Abuse Investigation Records) <input type="checkbox"/> Foster Care and Adoption Services Act (<u>MCL 722.954c</u> : Release of child's medical records, etc.) <input type="checkbox"/> Child Protection Law (MCL 722.623: Individual required to report child abuse or neglect, etc.)				
Other disclosures to law enforcement	<input type="checkbox"/> Uniform Crime Reporting System Act (<u>MCL 28.258</u> : Information for LEIN)			HIPAA (45 CFR 164.510, 164.512, 164.530) ; Patriot Act	
Research					
Disclosures for research	<input type="checkbox"/> Public Health Code (<u>MCL 333.2631</u> : Reporting or sharing research information with MDCH; <u>MCL 333.5703</u> : Toxicological studies of Vietnam veterans)			HIPAA (45 CFR 164.512, 164.514)	
Statutory Definitions					
Electronic Medical Record	<input type="checkbox"/> Child Protection Law (<u>MCL 722.627</u> : Central registry; availability of confidential records, etc.) <input type="checkbox"/> Michigan Penal Code (<u>MCL 750.492a</u> : Placing misleading or inaccurate information in medical records or charts; etc.) <input type="checkbox"/> Michigan Vehicle Code (<u>MCL 257.207a</u> : Electronic driver license status check, etc.)				

Electronic Health Record					
Health Information Exchange	<input type="checkbox"/> Public Health Code (MCL 333.2503: Health information technology commission; creation, etc.)				
Health Information Organization					
Personal Health Record					
Consent	<input type="checkbox"/> Rule 325.3828: Informed consent				
Authorization					
Privacy					
Confidentiality					

2.0 Describe plans to develop policies and procedures necessary to enable and foster information exchange within the state and interstate.

2.1 Interstate policies deal with the ability for the MiHIN Backbone to connect with the NHIN

2.2. Intrastate policies deal with the ability of Community HIEs to connect to the MiHIN Backbone

2.2.1 Patient consent:

Michigan began working on the individual consent issue during the MiHIN Conduit to Care project in 2006. The legal work group that was dually functioning as a resource for both the Conduit to Care Project and the ONC’s Health Information Security and Privacy Collaboration (HISPC) recommended that the State- through the MIHIN Resource Center, address individual consent. (see proposal in appendix 1.0)

A separate work group was formed, to address the issue and recommended an Informed Opt Out policy for individual consent for HIE, which was modeled after the Michigan Care Improvement Registry (MCIR) Opt Out model. Opt out was selected based on administrative efficiency, the general consensus about consumer comfort with opting out (based on Michigan survey results), and a discussion about how health information is currently shared.

The work group developed an Opt Out form (see appendix 1.1) and an initial process for allowing individuals to Opt Out- which included an online form. One of the major considerations for the work group was to ensure that individuals had a clear understanding of what “Opt Out” would mean. The work group decided that adding information about HIEs and how they exchanged information should be included in each participating provider’s Notice of Privacy Practices (NPP). Recommended language was drafted for participants to add to the NPP.

This recommendation was presented to the HIT Commission- who approved it unanimously in 2007

Form/Template for Opting Out The work group needs to review the form developed by the previous work group and make any necessary changes (see form in appendix)

De-Identified Data

Access of De-Identified Data for Specified Uses. For all individuals who do not elect to opt out, participant will be granted access to De-Identified Data via the MIHIN governed by Community HIE for the following purposes:

Research approved by an Institutional Review Board or Privacy Board organized and operating in accordance with 45 C.F.R. § 164;

Public health purposes, in accordance with 45 C.F.R § 164.512(b), or as authorized by other federal and state laws or regulations, including monitoring disease trends, conducting outbreak investigations, responding to public health emergencies, assessing the comparative effectiveness of medical treatments (including pharmaceuticals), conducting adverse drug event reporting, and informing new payment reforms; and

Evaluation and improvement of Community HIE operations, including analyses performed by the Community HIE, government agencies or their contractors.

Other Requirements.

All other uses of De-Identified Data shall require additional, separate Consent.

A Community HIE shall not condition a patient's participation in the RHIO on the patient's decision to consent or deny access to De-Identified Data for purposes other than those set forth in Section 1.6.1.

A Community HIEs shall, or shall require Participants to, comply with standards for the de-identification of data set forth in 45 C.F.R. § 164.514.

A Community HIEs shall, or shall require Participants to, subject any use of De-Identified Data to adequate restrictions on the re-identification of said data.

Sensitive health information

HL7 confidentiality codes- allow all sensitive data can be "tagged" or coded as such, in order to be restricted based on the patient's consent directive (or other). If all data is available in electronic form- and code, it can be managed and restricted until sometime in the future- when it will be ready for exchange.

This would include:

HIV AIDS

[MCL 333.5114; 333.16267 \(test results\)](#)
[MCL 333.5114a \(partner notification\)](#)
[MCL 333.5131 \(confidentiality\)](#)

STDS

Mental Health

[MCL 330.1748 \(confidentiality\)](#)
[MCL 333.6521 \(confidentiality\)](#)
[MCL 330.1946 \(duty to warn\)](#)

Substance Abuse

[MCL 333.6111 \(records of substance abuse treatment\)](#)
[MCL 333.6112; 333.6113 \(disclosures of substance abuse records\)](#)

Genetics

[MCL 500.3407b \(non-discrimination based on testing\)](#)
[MCL 333.17020 \(informed consent\)](#)
[MCL 333.17520 \(informed consent\)](#)
[MCL 550.1401\(3\)\(e\) \(nondisclosure of genetic test results\)](#)

Reproductive Health

[MCL 333.17015 \(informed consent for abortion\)](#)
[MCL 333.2834 \(fetal death\)](#)
[MCL 333.2835; 333.2837 \(abortion reporting\)](#)
[MCL 333.9132 \(minor capacity to consent\)](#)

Minors

[MCL 330.1707 \(mental health services\)](#)
[MCL 333.5127 \(HIV, STD\)](#)
[MCL 333.6121 \(substance abuse\)](#)

The age at which an individual is entitled to exercise privacy rights on his or her own behalf is determined as a matter of state law. While this is usually the age of 18, younger individuals may be entitled to exercise their own privacy rights where they are legally emancipated, or with respect to PHI regarding health care for which they otherwise have a legal right to make their own decisions. This may be the case in particular with respect to decisions about mental health and substance abuse care, abortion and contraception, and sexually transmitted diseases (STDs).

Break the glass

Affirmative Consent shall not be required for a Practitioner to access Patient Health Information via the MIHIN governed by a Community

HIE and the Practitioner may *Break the Glass* if the following conditions are met:

Treatment may be provided to the patient without informed consent as provided REFERENCE TO MICH LAW, i.e., in the Practitioner's judgment an emergency condition exists and the patient is in immediate need of medical attention and an attempt to secure consent would result in delay of treatment which would increase the risk to the patient's life or health.

The Practitioner determines, in his or her reasonable judgment, that information that may be held by or accessible via the MIHIN governed by a Community HIE may be material to emergency treatment.

The Practitioner attests that all of the foregoing conditions have been satisfied, and the Community HIE software maintains a record of this access.

Community HIEs shall ensure, or shall require their Participants to ensure, that access to information via the MIHIN governed by a Community HIE terminates upon the completion of the emergency treatment.

Notwithstanding anything to the contrary set forth in these policies, a Community HIE and its Participants shall not include any Sensitive Health Information from access via the MIHIN governed by a Community HIE.

Public health reporting

- 2.2.2 Authorization- see draft policy in appendix
- 2.2.3 Authentication- see draft policy in appendix
- 2.2.4 Access- see draft policy in appendix
- 2.2.5 Audit- see draft policy in appendix
- 2.2.6 Breach-

3.0 Describe plans to communicate and/or negotiate with other states to enable exchange

3.1 Outreach and leveraging relationships

4.0 Describe existing trust agreements that enable the secure flow of information among parties.

4.1 Survey of what exists

MCIR

UP

CARHIO

4.2 Draft Agreements for use by Community HIEs

4.2.0 Draft data use agreement

4.2.1 Draft data sharing agreement

4.2.2. Draft Business Associate Agreement

5.0 Describe stakeholder endorsement of the statewide policy framework

5.1 MIHIN Process

5.2 Organizations and entities that are on Board

- *HIT Commission*
- *MDCH*
- *MDIT*
- *Blue Cross Blue Shield*
- *Associations*
 - *MSMS*
 - *MHA*
 - *MOA*

6.0 Describe how the state will address issues of noncompliance with

6.1 Federal laws

HIPAA

HITECH

FERPA, etc. (will incorporate language into policies that enforce and defer to any federal laws and compliance/enforcement schemes)

6.2 State laws

- *Social Security Number Confidentiality Act*
- *Michigan's Identity Theft Protection Act (MCL 445.61 et seq.)*
- *State laws that are relevant (will incorporate into policies that enforce and will defer to any state laws and compliance schemes) Multiple state departments will have to work together regarding enforcement- for MDCH, will look to legal affairs*

Subject Matter

Michigan Laws

Purposes of HIE

Treatment

MCL 333.20201 (patient rights and responsibilities)

MCL 333.20201

MCL 333.16648 (information relative to dental care)

MCL 600.2157 (physician-patient privilege)

MCL 330.1746 (mental health records)

Public health

MCIR rules R 325.161 et seq.

(Proposed revision 6/27/07)

Cancer Reporting R 325.971

MCL 333.2221 (public health programs)

MCL 333.2611 (Confidentiality policies);

333.2631 et

seq.; 333.2821 (vital records);

MCL 333.5111 (prevention and control of disease)

MCL 333.5721 (reporting birth defects)

Research

MCL 333.2631 et seq. (department's use of data for

research purposes)

Law enforcement and bioterrorism

MCL 750.411 (injury reporting)

MCL 28.258 (Law Enforcement Information Network)

MCL 257.625a (driving while intoxicated)

MCL 333.2844a (dental records for missing persons)

Special Access Limitation

Reproductive health issues

MCL 333.17015 (informed consent for abortion)

MCL 333.2834 (fetal death)

MCL 333.2835; 333.2837 (abortion reporting)

MCL 333.9132 (minor capacity to consent)

Abuse and neglect issues

MCL 722.623 (child abuse)

MCL 333.2640 (provision of medical records)

MCL 330.1748a (mental health)

MCL 330.1723 (obligation to report)

Consent by minors to treatment without disclosure to parents

MCL 330.1707 (mental health services)

MCL 333.5127 (HIV, STD)

MCL 333.6121 (substance abuse)

HIV status

MCL 333.5114; 333.16267 (test results)

MCL 333.5114a (partner notification)

MCL 333.5131 (confidentiality)

Genetics

MCL 500.3407b (non-discrimination based on testing)

MCL 333.17020 (informed consent)

MCL 333.17520 (informed consent)

MCL 550.1401(3)(e) (nondisclosure of genetic test results)

Mental health and substance abuse	MCL 330.1748 (confidentiality) MCL 333.6521 (confidentiality) MCL 330.1946 (duty to warn) MCL 333.6111 (records of substance abuse treatment) MCL 333.6112; 333.6113 (disclosures of substance abuse records)
HIE Participants/Access	<i>MCL 15.243 (Michigan's FOIA exempts from disclosure privileged information, medical information w/ identifiers)</i> <i>MCL 333.20175 (facility records)</i> <i>MRAA, MCL 333.26261 et seq.</i> <i>MCL 333.16648 (dental records)</i> <i>MCL 333.16213 (practitioner records)</i> <i>MCL 333.17752 (prescription drug records)</i> <i>MCL 550.1406; 550.1604 (confidentiality obligations)</i> <i>MRAA, MCL 333.26261 et seq.</i> <i>MCL 722.30 (parents' right to information)</i> <i>MCL 333.16238 (confidentiality of information obtained in disciplinary investigation)</i> <i>MCL 333.16243 (information for disciplinary investigation)</i>
Payors Consumers Government	<i>Michigan's Identity Theft Protection Act (MCL 445.61 et seq.)</i>
Data Security	<i>MCL 333.16213; 333.20175 (record retention, confidentiality)</i> <i>MCL 333.16644 (dental records)</i> <i>MCL 400.111b (medical assistance programs)</i> <i>MCL 333.17753 (prescription processing)</i> <i>R 338.471a et seq. (Board of Pharmacy rules)</i>
Record Retention Requirements	<i>MCL 333.21773 (involuntary transfers from nursing homes)</i> <i>MCL 333.20201 (patient rights and responsibilities)</i>
Pharmacy Issues	<i>MCL 333.16221 (investigation of licensee)</i> <i>MCL 333.16221</i>
Limit liability	Donated Technology Donation of technology, ongoing support Update of Michigan disciplinary law re Stark II
Discovery & Evidentiary Record retention	<i>MCR 2.314; 2.506 (court rules on subpoenas, discovery)</i> <i>Michigan peer review laws (MCL 331.531)</i> <i>Public Health Code (e.g., records retention under MCL 333.16213; 333.20175)</i> <i>MCL 333.17753 (prescription processing)</i> <i>R 338.471a et seq. (Board of Pharmacy rules)</i> <i>MCL 450.831 et seq. (Uniform Electronic Transactions Act)</i>
E-Sign issues	

6.3 State HIE policies

- *Will enforce policies and procedures via privacy and security officer named as the compliance staff for the MiHIN and will have to work with the same officers in the community HIEs. Also will work with Regional ONC Privacy Officer. Enforcement will be regulated by overseeing body of MiHIN by leveraging connection to MiHIN Backbone.*

Appendix

INDIVIDUAL ACCESS

Individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format.

Access to information enables individuals to manage their health care and well-being. Individuals should have a reasonable means of access to their individually identifiable health information. Individuals should be able to obtain this information easily, consistent with security needs for authentication of the individual; and such information should be provided promptly so as to be useful for managing their health. Additionally, the persons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, should provide such information in a readable form and format, including an electronic format, when appropriate. In limited instances, medical or other circumstances may result in the appropriate denial of individual access to their health information.

CORRECTION

Individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information, and to have erroneous information corrected or to have a dispute documented if their requests are denied.

Individuals have an important stake in the accuracy and integrity of their individually identifiable health information and an important role to play in ensuring its accuracy and integrity. Electronic exchange of individually identifiable health information may improve care and reduce adverse events. However, any errors or conclusions drawn from erroneous data may be easily communicated or replicated (e.g., as a result of an administrative error as simple as a transposed digit or more complex error arising from medical identity theft). For this reason it is essential for individuals to have practical, efficient, and timely means for disputing the accuracy or integrity of their individually identifiable health information, to have this information corrected, or a dispute documented when their requests are denied, and to have the correction or dispute communicated to others with whom the underlying information has been shared. Persons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, should make processes available to empower individuals to exercise a role in managing their individually identifiable health information and should correct information or document disputes in a timely fashion.

OPENNESS AND TRANSPARENCY

There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their individually identifiable health information.

Trust in electronic exchange of individually identifiable health information can best be established in an open and transparent environment. Individuals should be able to understand what individually identifiable health information exists about them, how that individually identifiable health information is collected, used, and disclosed and whether and how they can exercise

choice over such collections, uses, and disclosures. Persons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, should provide reasonable opportunities for individuals to review who has accessed their individually identifiable health information or to whom it has been disclosed, in a readable form and format. Notice of policies, procedures, and technology-- including what information will be provided under what circumstances -- should be timely and, wherever possible, made in advance of the collection, use, and/or disclosure of individually identifiable health information. Policies and procedures developed consistent with this Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information should be communicated in a manner that is appropriate and understandable to individuals.

INDIVIDUAL CHOICE

Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable health information.

The ability of individuals to make choices with respect to electronic exchange of individually identifiable health information concerning them is important to building trust. Persons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, should provide reasonable opportunities and capabilities for individuals to exercise choice with respect to their individually identifiable health information. The degree of choice made available may vary with the type of information being exchanged, the purpose of the exchange, and the recipient of the information. Applicable law, population health needs, medical necessity, ethical principles, and technology, among other factors, may affect options for expressing choice. Individuals should be able to designate someone else, such as a family member, care-giver, or legal guardian, to make decisions on their behalf. When an individual exercises choice, including the ability to designate someone else to make decisions on his or her behalf, the process should be fair and not unduly burdensome.

COLLECTION, USE, AND DISCLOSURE LIMITATION

Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately.

Establishing appropriate limits on the type and amount of information collected, used, and/or disclosed increases privacy protections and is essential to building trust in electronic exchange of individually identifiable health information because it minimizes potential misuse and abuse. Persons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, should only collect, use, and/or disclose information necessary to accomplish a specified purpose(s). Persons and entities should take advantage of technological advances to limit data collection, use, and/or disclosure.

DATA QUALITY AND INTEGRITY

Persons and entities should take reasonable steps to ensure that individually identifiable health information is complete, accurate, and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner.

The completeness and accuracy of an individual's health information may affect, among other things, the quality of care that the individual receives, medical decisions, and health outcomes.

Persons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, have a responsibility to maintain individually identifiable health information that is useful for its intended purposes, which involves taking reasonable steps to ensure that information is accurate, complete, and up-to-date, and has not been altered or destroyed in an unauthorized manner. Persons and entities have a responsibility to update or correct individually identifiable health information and to provide timely notice of these changes to others with whom the underlying information has been shared. Moreover, persons and entities should develop processes to detect, prevent, and mitigate any unauthorized changes to, or deletions of, individually identifiable health information.

SAFEGUARDS

Individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.

Trust in electronic exchange of individually identifiable health information can only be achieved if reasonable administrative, technical, and physical safeguards are in place to protect individually identifiable health information and minimize the risks of unauthorized or inappropriate access, use, or disclosure. These safeguards should be developed after a thorough assessment to determine any risks or vulnerabilities to individually identifiable health information. Persons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, should implement administrative, technical, and physical safeguards to protect information, including assuring that only authorized persons and entities and employees of such persons or entities have access to individually identifiable health information. Administrative, technical, and physical safeguards should be reasonable in scope and balanced with the need for access to individually identifiable health information.

ACCOUNTABILITY

These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.

These nationwide privacy and security principles will not be effective in building trust in electronic exchange of individually identifiable health information unless there is compliance with these Principles and enforcement mechanisms. Mechanisms for assuring accountability include policies and procedures and other tools. At a minimum, such mechanisms adopted by persons and entities, that participate in a network for the purpose of electronic exchange of individually identifiable health information, should address: (1) monitoring for internal compliance including authentication and authorizations for access to or disclosure of individually identifiable health information; (2) the ability to receive and act on complaints, including taking corrective measures; and (3) the provision of reasonable mitigation measures, including notice to individuals of privacy violations or security breaches that pose substantial risk of harm to such individuals.ⁱ

ⁱ Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information, Office of the National Coordinator for Health Information Technology U.S. Department of Health and Human Services. Dec. 15, 2008

Instructions: Check the appropriate boxes and complete the Individual Information, Individual or Parent/Guardian Signature and Contact Information sections.

.....

Request to Opt-Out

I want to limit the electronic exchange and display of my Protected Health Information (PHI) that is transmitted to my other health care providers, health plans and insurers by the Michigan Health Information Network (MiHIN). By completing and signing this form, I understand the following:

I understand the purpose of the MiHIN is to increase the timeliness and improve the quality of my medical treatment. I understand that in the event of an emergency, health care providers may have access to my PHI through the MiHIN during the emergency.

.....

Individual Information

Name _____			
Last	First	Middle	
Date of Birth _____	Home Address: _____		
(MM/DD/YYYY)	_____		

Individual or Parent/Guardian Signature and Contact Information

Name _____			
Last	First	Middle	
Relationship to Minor _____		Phone Number _____	
Signature _____		Date _____	

.....

Request to Terminate my choice to Opt-Out.

I want to reverse my choice to not share my PHI electronically though the MiHIN. By completing and signing this form, I understand all of my PHI may be accessible to my health care providers, health plans and insurers unless restricted by applicable state or federal laws.

Proposal to Implement the MiHIN Informed Opt-Out Policy for Consumers

Background

The MiHIN legal workgroup, combined with a Health Information Security and Privacy Collaboration (HISPC) presented a list of recommendations to the Health Information Technology Commission at its December 13, 2007 meeting. Among the recommendations the commission adopted was the idea to “establish informed opt-out as the method of consumer control of how their protected health information becomes part of the HIE.” Similar policies are used by the Michigan Care Improvement Registry (MCIR) and by other health information exchanges across the country.

The challenge then became to find the best means to implement the policy. Since providers and insurers routinely distribute “Notice of Privacy Practices” (NPP) as required by HIPAA, one suggestion was to use this document as a vehicle to inform consumers about MiHIN and their right to “opt out” (essentially block download of their protected health information). A Privacy and Consent work group was convened by the MiHIN Resource Center in summer 2008 to discuss this idea and the proposed NPP language. A representative group of consumers, medical professionals, privacy officers, regional representatives, and attorneys participated. During the September 2008 meeting HIT Commission, members discussed the informed opt-out process and asked the Resource Center staff to explore the issue further. Participants in an October meeting that included attorneys representing two of the stakeholder groups on the commission refined this idea further.

Proposal

The outcome of this process is a proposal to implement the informed opt-out process through a simple statement in the Notice of Privacy Practices (NPP) used by participating organizations and through the distribution of consumer education materials. Parties exchanging protected health information through a MiHIN health information exchange will be asked to include statements such as the one below in their NPPs and other appropriate documents:

Sample Language for Notice of Privacy Practices

“This organization participates in the Michigan Health Information Network (MiHIN). For more information about MiHIN and your right to limit the display of your protected health information to other MiHIN participants, please see www.mihin.org, call 1-800-XXX-XXXX, or write to MiHIN, P.O. Box XX, Lansing, MI 488XX.”

The Resource Center will create and update consumer education materials using the suggestions from the privacy and consent workgroup and other key stakeholders. Originally we had proposed to include more extensive language in the NPP, but after further discussion it became apparent that this might not have the desired effects because 1.) consumers rarely read NPPs and 2.) any material changes to NPP language might prompt legal review by participating providers and lead to inconsistent language adoption across the state. By keeping the notice simple and creating separate consumer communications, MiHIN will have the flexibility to adapt messages as necessary. One suggestion that came out of the privacy and consent work group, for example, was to create education materials and consent forms for consumers of community mental health services. We are following up on this suggestion and hope to pilot it in the CARHIO region.

The Resource Center has also been organizing an internal State of Michigan work group to examine the implementation of a master patient index / record locator service (the “MiHIN Hub”) to connect the nine MiHIN regions to each other, state government systems, and possibly other sources. We propose that the hub include a consent management database to identify consumers who have opted-out. More detailed procedures still need to be determined, but if the concept is approved it will help both the state and the MiHIN regions to anticipate the process with their vendors and health information exchange participants.

AUTHORIZATION

Purpose/Principles

Authorization is the process of determining whether a particular individual within a Participant has the right to access Protected Health Information via the MIHIN governed by a Community HIE. Authorization is based on 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 Participant. This Section 2 sets forth minimum requirements that Community HIE and their Participants shall follow when establishing role-based access standards and authorizing individuals to access information about a patient via the MIHIN governed by a Community HIE. They are designed to limit exchange of information to the minimum necessary for accomplishing the intended purpose of the exchange, thereby allowing patients to have confidence in the privacy of their health information as it moves among Participants in a Community HIE.

Policies and Procedures

1.1 Role-Based Access Standards.

1.1.1 Community HIE shall establish and implement policies and procedures that:

- a. Establish categories of Authorized Users;
- b. Define the purposes for which Authorized Users in those categories may access Protected Health Information via the MIHIN governed by a Community HIE; and
- c. Define the types of Protected Health Information that Authorized Users within such categories may access (e.g., demographic data only, clinical data).

1.1.2 The purposes for which an Authorized User may access information via the MIHIN governed by a Community HIE and the types of information an Authorized User may access shall be based, at a minimum, on the Authorized User's job function and relationship to the patient.

1.1.3 At a minimum, Community HIE 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:

- a. Practitioner with access to clinical information and Break the Glass authority;
- b. Practitioner with access to clinical information but no Break the Glass authority;
- c. Non-Practitioner with access to clinical information;
- d. Non-Practitioner with access to non-clinical information;
- e. Community HIE administrators with access to non-clinical information; and

-
- f. Community HIE administrators with access to clinical information in order to engage in public health reporting purposes in accordance with Section 1.2.2 of these Policies.

1.1.4 Community HIE shall require Participants to designate the individuals within their organizations who will be authorized to access information via the MIHIN governed by a Community HIE and to assign those individuals to the appropriate categories as listed above.

DRAFT

AUTHENTICATION

Purpose/Principles

Authentication is the process of verifying that an individual who has been authorized and is seeking to access information via the MIHIN governed by a Community HIE is who he or she claims to be. This is accomplished by providing proof of identity. This Section 3 sets forth minimum requirements that Community HIE and their Participants shall follow when authenticating individuals prior to allowing them to access information via the MIHIN governed by a Community HIE. These Policies and Procedures represent an important technical security safeguard for protecting a patient's information from various internal and external risks, including unauthorized access.

Policies and Procedures

1.2 **Obligation to Ensure Authentication of Identity of Authorized User Prior to Access.**

Community HIE shall authenticate, or shall require their Participants to authenticate, each Authorized User's identity prior to providing such Authorized User with access to Protected Health Information via the MIHIN governed by a Community HIE. Such authentication shall take place in accordance with the provisions of this Section 3.

1.3 **Authentication Requirements.**

1.3.1 Transitional Authentication Standard. Until such time as a determination is made, pursuant to Section 3.2.2, to utilize a higher authentication standard, Community HIE shall authenticate, or shall require their Participants to authenticate, each Authorized User through an authentication methodology that meets the minimum technical requirements for Authentication Assurance Level 2 ("Level 2") set forth in National Institute of Standards and Technology Special Publication 800-63 (hereinafter, "NIST SP 800-63").

- a. Level 2 will require, among other technical specifications, Community HIE or their Participants to authenticate each Authorized User's identity using only single-factor authentication, which queries Authorized Users for something they know (e.g., a password). Under Level 2, Community HIE or their Participants will be free to use only a password, and need not use it in combination with any other tokens, provided it protects against online guessing and replay attacks. Level 2 will require Community HIEs or their Participants to implement initial identity-proofing procedures (either remote or in-person) that require Authorized Users to provide identifying materials and information upon application for access to information through the Community HIE.

1.3.2 Minimum Authentication Standard. In light of the importance of strong security measures to the protection of patient data and the transition of certain organizations and entities, including but not limited to the Michigan State Medicaid Program, toward utilization of an authentication methodology that meets the minimum technical requirements for Authentication Assurance Level 3 ("Level 3") set forth in NIST SP 800-63, Community HIE shall be required to authenticate, or require their Participants to authenticate, each Authorized User through an authentication methodology that meets the minimum technical requirements for Level 3. The MIHIN governing entity shall establish a Work Group to

consider the cost, workflow, and other issues implicated by a transition to Level 3, and determine the implementation approach and timetable for transition to Level 3.

- a. Level 3 will require, among other technical specifications, Community HIE or their Participants to authenticate each Authorized User's identity using multifactor authentication, which queries Authorized Users for something they know (e.g., a password) *and* something they have (e.g., an ID badge or a cryptographic key). Community HIE or their Participants will be free to use a combination of tokens (authentication secrets to which an Authorized User's identity is bound), including soft cryptographic tokens with the key stored on a general-purpose computer, hard cryptographic tokens, which have the key stored on a special hardware device like a key FOB, or one-time password device tokens, which have a symmetric key stored on a personal hardware device (e.g., a cell phone) in a manner that protects against protocol threats, including eavesdropper, replay, online guessing, verifier impersonation, and man-in-the-middle attacks. In addition to use of multifactor authentication, Level 3 will require Community HIE or their Participants to implement initial identity-proofing procedures (either remote or in person) that require Authorized Users to provide identifying materials and information (e.g., a valid current primary Government Picture ID and either address of record or nationality, such as a driver's license or passport) upon application for access to information through the Community HIE though these requirements will be more stringent than those set forth at Level 2.

1.3.3 Choice of Technical Solution. In meeting the requirements set forth in this Section 3.2, Community HIE and their Participants may select the best available authentication methodology, consistent with guidance set forth in NIST SP 800-63, based on individual assessments of their technical architectures, network sizes, and policies.

1.4 Compliance with Policies Resulting from Statewide Risk Analysis. In the event that Michigan conducts a statewide risk analysis of the potential harm and likelihood of adverse impacts that could result from an error in identity authentication within the MIHIN that indicates that authentication policies and procedures that differ from, or are in addition to, those set forth in this Section 3, should be adopted, any such authentication policies and procedures shall be developed and approved through the SCP before adoption.

1.5 Option to Rely on Statewide Authentication Service. In the event that Michigan develops statewide services for the authentication of Authorized Users, Community HIE may utilize such statewide services to authenticate an Authorized User in accordance with the provisions of this Section 3.

ACCESS

Purpose/Principles

Access controls govern when and how a patient's information may be accessed by individuals within a Community HIE's Participant. This Section 4 sets forth minimum behavioral controls Community HIEs shall implement to ensure that: 1.) only Authorized Users access information via the MIHIN governed by a Community HIE; and 2.) they do so only in accordance with patient consent and with other requirements (specified herein) that limit their access to specified information (e.g., that which is relevant to a patient's treatment). These access policies, coupled with informed patient consent, are designed to reduce unauthorized access and ensure information is used for authorized purposes.

Policies and Procedures

- 1.6 General.** Community HIE shall, or shall require their Participants to, ensure that each Authorized User is assigned a unique user name and password to provide such Authorized User with access to patient information via the MIHIN governed by a Community HIE. In doing so, Community HIEs and/or their Participants shall comply with the following minimum standards:
- 1.6.1** Authorized Users shall be authenticated in accordance with the provisions of Section 3.
 - 1.6.2** 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).
 - 1.6.3** Group or temporary user names shall be prohibited.
 - 1.6.4** Authorized Users shall be required to change their passwords at least every 90 calendar days and shall be prohibited from reusing passwords.
 - 1.6.5** 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.
- 1.7 Authorized Purposes.** Community HIEs and their Participants shall permit Authorized Users to access Protected Health Information of a patient via the MIHIN governed by a Community HIE only for purposes consistent with a patient's Affirmative Consent.
- 1.8 Failed Access Attempts.** Community HIEs shall enforce a limit of consecutive Failed Access Attempts by an Authorized User. Upon a fifth Failed Access Attempt, Community HIEs shall ensure that said Authorized User's access to the Community HIE is disabled either by locking the account until release by a Community HIE administrator or by locking the account for a specific period of time as specified by the Community HIE, after which the Authorized User may reestablish access using appropriate identification and authentication procedures.
- 1.9 Periods of Inactivity.** Community HIEs shall ensure that an Authorized User is automatically logged out of the Community HIE after a period of inactivity by such Authorized User. The termination shall remain in effect until the Authorized User reestablishes access using appropriate identification and authentication procedures. Community HIEs shall establish the length of periods of inactivity that will trigger such termination based on their internal risk analyses as well

organizational factors such as current technical infrastructure, hardware and software security capabilities.

- 1.10 Access Limited to Minimum Necessary Information.** Community HIEs shall, and shall require their Participants to, ensure that reasonable efforts are made, except in the case of access for Treatment, to limit the information accessed via the MIHIN governed by a Community HIE to the minimum amount necessary to accomplish the intended purpose for which the information is accessed.
- 1.11 Record Locator Service and Other Comparable Directories.** In operating a Record Locator Service or Other Comparable Directory, Community HIEs shall, or shall require their Participants to:
- 1.11.1** Implement reasonable safeguards to minimize Incidental Disclosures during the process of identifying a patient and locating a patient's medical records.
 - 1.11.2** Prohibit Authorized Users from accessing Protected Health Information in any manner inconsistent with these Policies and Procedures
- 1.12 Training.** The behavioral and organizational access controls set forth above will only be effective if 1) a Community HIE's health information access policies and procedures are clear; and 2) Authorized Users understand the policies and procedures and their responsibilities within such policies and procedures. As such, Community HIEs shall develop and implement, either directly or through Participants, minimum training requirements for educating individuals about the policies and procedures for accessing Protected Health Information via the MIHIN governed by a Community HIE.
- 1.12.1** Community HIEs shall, or shall require their Participants to, provide either on-site training, web-based training, or comparable training tools so that Authorized Users are familiar with the operation of the Community HIE and the policies and procedures governing access to information via the MIHIN governed by a Community HIE.
 - 1.12.2** Community HIEs shall, or shall require their Participants to, ensure that each Authorized User undergoes such training prior to being granted access to information via the MIHIN governed by a Community HIE.
 - 1.12.3** Community HIEs shall, or shall require their Participants to, ensure that each Authorized User signs a certification that he or she has received training and will comply with the Community HIE's policies and procedures. Such certification shall be retained by Community HIEs or their Participants for at least six years.
 - 1.12.4** Community HIEs may, but shall not be required to, ensure that each Authorized User undergo continuing and/or refresher training on a periodic basis as a condition of maintaining authorization to access patient information via the MIHIN governed by a Community HIE.
- 1.13 Termination of Access and Other Sanctions.** Community HIEs shall develop policies and procedures to terminate, or to require their Participants to terminate, the access of Authorized Users and/or to impose sanctions as necessary.

-
- 1.13.1** Community HIEs shall ensure that access to the Community HIE of a Participant (and all of the Participant's Authorized Users, if applicable) is terminated in the following situations and in accordance with the processes described:
- a. Immediately or as promptly as reasonably practicable but in any event within one business day of termination of a Participant's Participation Agreement with the Community HIE; and/or
 - b. Immediately or as promptly as reasonably practicable but in any event within one business day of notification of termination of an Authorized User's employment or affiliation with the Participant.
- 1.13.2** In order to comply with Section #####, Community HIEs shall require their Participants to notify the Community HIE upon termination of an Authorized User's employment or affiliation with the Participant immediately or as promptly as reasonably practicable but in any event within one business day of termination.
- 1.13.3** Community HIEs shall establish sanctions to redress policy or procedural violations. Sanctions could include temporary access prohibitions, re-training requirements, termination, or other processes the Community HIE deems necessary in accordance with its internal risk analyses.
- 1.13.4** The MIHIN Governing Body shall develop guidance on the following to be included in V2.0 of these Policies and Procedures: 1.) How Community HIEs should respond to discovery requests and subpoenas; 2.) Whether state-level sanctions should be developed and implemented by Community HIEs.

Audit

Purpose/Principles

Audits are useful oversight tools for recording and examining access to information through a Community HIE (e.g., who accessed what data and when) and are necessary for verifying compliance with access controls, like those specified in Section 4, developed to prevent/limit inappropriate access to information. This Section 6 sets forth minimum requirement that Community HIEs and their Participants shall follow when logging and auditing access to health information via the MIHIN governed by a Community HIE.

Policies and Procedures

1.14 Maintenance of Audit Logs. Each Community HIE shall maintain Audit Logs that document all access of Protected Health Information via the MIHIN governed by a Community HIE.

1.14.1 Audit Logs shall, at a minimum, include the following information:

- a. The identity of the patient whose Protected Health Information was accessed;
- b. The identity of the Authorized User accessing the Protected Health Information;
- c. The identity of the Participant with which such Authorized User is affiliated;
- d. The type of Protected Health Information or record accessed (e.g., pharmacy data, laboratory data, etc.);
- e. The date and time of access;
- f. The source of the Protected Health Information (i.e., the identity of the Participant from whose records the accessed Protected Health Information was derived); and
- g. Unsuccessful access (log-in) attempts.

1.14.2 Audit Logs shall be immutable. An immutable Audit Log requires either that log information cannot be altered by anyone regardless of access privilege or that any alterations are tamper evident.

1.14.3 Audit Logs shall be maintained for a period of at least six years from the date on which information is accessed.

1.15 Obligation to Conduct Periodic Audits. Each Community HIE shall conduct, or shall require each of its Participants to conduct, periodic audits to monitor use of the Community HIE by Participants and their Authorized Users and ensure compliance with Policies and Procedures and all applicable laws, rules and regulations.

1.15.1 At a minimum, the Community HIE shall audit, or require its Participants to audit, the following:

-
- a. That Affirmative Consents are on file for patients whose Protected Health Information is accessed via the MIHIN governed by a Community HIE, other than in Break the Glass situations;
 - b. That Authorized Users who access Protected Health Information via the MIHIN governed by a Community HIE do so for Authorized Purposes; and
 - c. That applicable requirements were met where Protected Health Information was accessed through the Break the Glass function.
- 1.15.2** The activities of all or a statistically significant subset of a Community HIE's Participants shall be audited.
- 1.15.3** Periodic audits shall be conducted at least on an annual basis. Community HIEs shall consider their own risk analyses and organizational factors, such as current technical infrastructure, hardware and software security capabilities, to determine the reasonable and appropriate frequency with which to conduct audits more often than annually.
- 1.15.4** Periodic audits shall be conducted using a statistically significant sample size.
- 1.15.5** If audits are conducted by Participants rather than by the Community HIE, the Community HIE shall:
- a. Require each Participant to conduct the audit within such time period as reasonably requested by the Community HIE; and
 - b. Require each Participant to report the results of the audit to the Community HIE within such time period and in such format as reasonably requested by the Community HIE.
- 1.16 Participant Access to Audit Logs.**
- 1.16.1** A Community HIE shall provide the Participant, upon request, with the following information regarding any patient of the Participant whose Protected Health Information was accessed via the MIHIN governed by a Community HIE:
- a. The name of each Authorized User who accessed such patient's Protected Health Information in the prior 6-year period;
 - b. The time and date of such access; and
 - c. The type of Protected Health Information or record that was accessed (e.g., clinical data, laboratory data, etc.).
- 1.16.2** A Participant shall only be entitled to receive audit log information pursuant to Section 6.3.1 for patients who have not opted out for that Participant to access his or her Protected Health Information.
- 1.16.3** Community HIEs shall provide such information as promptly as reasonably practicable but in no event more than 10 calendar days after receipt of the request

1.17 Patient Access to Audit Information.

1.17.1 Each Community HIE shall, or shall require its Participants to, provide patients, upon request, with the following information:

- a. The name and role (e.g., physician) of each Authorized User who accessed a patient's Protected Health Information in the prior 6-year period;
- b. The Participant through which such Authorized User accessed such Protected Health Information;
- c. The time and date of such access; and
- d. The type of Protected Health Information or record that was accessed (e.g., clinical data, laboratory data, etc.).

1.17.2 Community HIEs shall, or shall require their Participants to provide such information as promptly as reasonably practicable but in no event more than ten calendar days after receipt of the request.

1.17.3 If requested, Community HIEs shall, or shall require their Participants to, provide such information to patients at no cost once in every 12-month period. Community HIEs may establish a reasonable fee for any additional requests within a given 12-month period; provided that the Community HIE shall waive any such fee where such additional request is based on a reasonable suspicion of unauthorized access to the patient's Protected Health Information via the MIHIN governed by a Community HIE.

1.17.4 If applicable, Community HIEs shall, or shall require their Participants to, provide notice of the availability of such information on any patient portals maintained by the Community HIE or its Participants.

1.18 Public Availability of Audits. Each Community HIE shall make the results of its periodic audit available on the Community HIE's website. Such results shall be made available as promptly as reasonably practicable, but in any event not more than 30 days after completion of the audit.

MIHIN Community HIE Security Policies

This Security Policy for the Michigan Health Information Network ("MIHIN") will permit Community HIEs to operate in compliance with applicable laws governing computer security, and support the computer security obligations of those participating in the MIHIN. MIHIN, its vendors, participants and authorized users will strive to prevent any breaches in security and implement measures to promote the confidentiality of patient health information. Individually identifiable health information will be protected with reasonable administrative, technical and physical safeguards to enable its confidentiality, integrity and availability and to prevent unauthorized and inappropriate access, use or disclosure.

Appropriate computer security practices will be implemented by the MIHIN and each entity that exchanges data through the MIHIN (collectively, the "Participants"). Each Participant will develop and implement appropriate computer security policies and procedures. This policy is intended to complement the policies and procedures of each Participant. Each Participant shall have developed and implemented policies and procedures necessary or appropriate to comply with the requirements of the Security Standards of HIPAA, as well as other applicable computer security requirements. Such policies may include:

- Risk Analysis
- Risk Management
- Audit Controls
- Information System Activity Review
- Access Controls – Automatic Logoff/ Login Monitoring
- Access Controls – Person or Entity Authentication
- Workforce Security – Pre-access Workforce Clearance Procedures
- Workforce Security – Authorization and Supervision
- Workforce Security – Access Management
- Workforce Security – Training and Security Reminders
- Workforce Security – Sanction Policy
- Workforce Security – Termination Policy
- System Security – Encryption
- System Security – Facility Physical Security Plan
- System Security – Facility Contingency Operations
- System Security – Maintenance Records
- System Security – Workstation Use
- System Security – Device and Media Controls on Usage, Encryption and Disposal
- System Security – Protection from Malicious Software
- System Security – Contingency Plan/ Data Backup Plan/ Disaster Recovery Plan
- System Security – Risk Analysis
- Security Incident Procedures – Response and Reporting

Additional contractual obligations may be imposed on each Participant through the MIHIN Data Sharing Agreement and the Policies and Procedures implemented by the MIHIN. The Executive Committee may, but is not required to, provide guidance to the Participants on methods of compliance with HIPAA and the access agreements. The Executive Committee may also recommend whether a Participant's access to the

MIHIN represents a substantial risk to the security of the personal health information (PHI), and whether such Participant's access to PHI should be suspended.

This Policy sets forth the basic security requirements of the MIHIN. The role of the MIHIN is to (a) restrict access to PHI to Authorized Users only, (b) assist Participants in ensuring the confidentiality, integrity and availability of electronic PHI transmitted via the MIHIN; and (c) support patient privacy and the protection of the confidentiality of clinical and business information. Specifically, this policy is intended to:

- Support the actions taken by each Participant to reasonably protect Participants' applications, computer systems, networks, and electronic data ("Participants' Systems") from intentional and unintentional damage by providing a framework for developing, maintaining and monitoring compliance with security procedures;
- Reasonably protect the confidentiality, integrity and availability of Participants' electronic PHI in compliance with the Security Rule (45. CFR §164.302 *et seq.*) while the electronic PHI is within the possession and/or control of the RHIO; and
- Reasonably minimize the potential exposure to the MIHIN, Participants and their affiliates for damages which may result from unauthorized use of MIHIN or Participant systems or system data. Potential damages include, but are not limited to, the loss and/or unauthorized modification of electronic PHI, confidential health system data, or intellectual property, damage to public image, damage to critical RHIO internal systems, fines, civil monetary penalties and criminal penalties.

Definitions:

As used throughout this Policy, the capitalized terms shall have the following meaning:

"Authorized Users" shall have the meaning set forth in the Data Sharing Agreement.

"Electronic Protected Health Information" or "electronic PHI" means individually identifiable health information that is transmitted by or maintained in electronic media.

"Workforce Members" means Authorized Users, employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the RHIO or Participant.

"Workstation" means a computer monitor or other device which permits a Workforce Member to access electronic PHI and/or to use, send or transmit electronic PHI sent via the RHIO.

"Participant" has the meaning set forth in the Data Sharing Agreement.

"MIHIN" means the Capital Area Health Information Organization, a health information exchange organization.

MIHIN SECURITY POLICY 001: RISK ANALYSIS

Policy:

The Community HIE will conduct an assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI that is in the possession of or under the control of Community HIE. The risk analysis will consider potential losses caused by unauthorized uses and disclosures, whether intentional or unintentional, and any adverse impact on the confidentiality, availability or integrity of data that might reasonably be expected to occur if security measures are not implemented.

Procedure:

1. MIHIN recognizes the potential for exposing electronic PHI during the performance of its business operations. Exposures can occur during the creation, accessing, storing, and transmission of electronic PHI.
2. MIHIN will perform a Risk Analysis that will include the following:
 - Identification of the assets (i.e., hardware, software, system interfaces, data, etc.) used, owned or controlled by the MIHIN that contain, transmit or store electronic PHI.
 - Determination of threats and vulnerabilities to those assets (i.e., unauthorized access, destruction, alteration, natural disasters, etc). A quantitative or a qualitative methodology may be used.
 - Identification of potential safeguards against those threats and vulnerabilities.
 - A cost-benefit analysis by comparing the potential threat or vulnerability to the cost to safeguard against the threat or vulnerability.
3. Each Participant shall cooperate with the MIHIN in conducting the risk analysis, through reasonable sharing of information regarding the Participant's data sharing and security procedures. The MIHIN shall treat information regarding Participant data sharing and security procedures as confidential information.
4. **Asset Identification**
Each asset that creates, stores, or transmits electronic PHI will be identified.
5. **Threat and Vulnerability Analysis**
 - Each identified electronic PHI asset will be analyzed for any potential vulnerability to the integrity, confidentiality, and availability of its electronic PHI. The MIHIN will determine the levels of risk for the electronic PHI asset.
 - All electronic PHI assets will be assessed for the consequences arising from an undesirable event (i.e. catastrophic or minor) and the likelihood (i.e., occurs every year or almost never) of the risk occurring.
 - A list of threats and vulnerabilities with associated assets, the consequences, and the likelihoods of those consequences will be generated.
6. **Control Analysis**
 - Each threat and vulnerability will be examined for potential controls or safeguards to mitigate the risk. Threats and vulnerabilities can be mitigated by non-technical controls, technical controls, or a combination of the two.
 - A list of the threats and vulnerabilities with potential safeguards and/or controls will be generated.
7. **Cost Benefit Analysis**

-
- After completion of the Asset Identification, Threat and Vulnerability Analysis and Control Analysis, the MIHIN will perform a cost-benefit analysis to determine if the cost of the safeguard(s) and/or control(s) is cost effective for the value of the asset and the risks identified.
8. The MIHIN will assimilate the results of the Asset Identification, Threat and Vulnerability Analysis, Control Analysis and the Cost Benefit Analysis into a Risk Analysis report for presentation to the Participants indicating which safeguards and controls it intends to implement.
 9. Documentation generated from the Risk Analysis will be maintained for six years from the date of creation or from the date it was last in effect.
 10. The MIHIN may enlist assistance from Participants that may be necessary to complete this Risk Analysis. This may require coordination among Participant's departments such as Information Technology, Administration, and Human Resources.

References:

1. 45 CFR Parts 160 and 164: Health Insurance Reform: Security Standards; Final Regulations. National Institute of Standards and Technology, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security

MIHIN SECURITY POLICY 002: AUTHORIZATION

Policy:

Only trained and authorized users are permitted to access data through the system. MIHIN and its Participants will create categories of authorized users that define the purpose for which access may be granted and the types of Protected Health Information accessible for each category.

Procedure:

1. MIHIN will work with its technology vendor(s) to establish categories of user access based on the user's job function, relationship to the patient, and other factors approved by the Executive Committee.
2. Participants will designate particular individuals within their organizations who are authorized to access information via MIHIN and assign those individuals to the appropriate categories established by MIHIN above.
3. Authorized users will be unable to query MIHIN for information concerning patients who have requested to opt out of participation in MIHIN except when they "Break the Glass" under the following circumstances:
 1. The authorized user, in his or her professional judgment, has determined that the patient is in need of emergency treatment, and
 2. The patient is unable to remove his or her opt-out status before a delay of treatment would increase the risk to the patient's health.

Capital Area will maintain records of "Break the Glass" emergency access. (See Privacy Policy 010).

MIHIN SECURITY POLICY 003: PERSON OR ENTITY AUTHENTICATION

Policy:

The MIHIN and all Participants will implement procedures to verify that an Authorized User or entity seeking access to electronic Protected Health Information is the person or entity he/she/it claims to be.

Procedure:

1. All Participants shall implement and enforce a user authentication mechanism.
2. Each Authorized User seeking access to electronic PHI transmitted or stored by the RHIO shall utilize a user authentication mechanism to access the RHIO.
3. The authentication mechanism will be composed of an unique user identification and a token.
4. The unique user identification will be username.
5. The following tokens may be used to provide user authentication:
 - Passwords;
 - Smart cards;
 - Digital certificates; or
 - Other means approved by the MIHIN.
6. 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.
7. Authorized Users may not share or disclose to others their user authentication information.

References:

1. 45 CFR Parts 160 and 164: Health Insurance Reform: Security Standards; Final Regulations.
2. National Institute of Standards and Technology, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

MIHIN SECURITY POLICY 004: SYSTEM SECURITY

Policy:

The MIHIN and the Participants will implement and/or maintain physical security policies, procedures and guidelines for all hardware used in connection with the MIHIN system, including workstations. Policies and procedures will address attributes such as the placement and protection of equipment and how the Authorized Users will perform the appropriate functions.

Procedure:

1. Authorized Users may use a workstation or other remote access mechanism to create, access, store, and transmit electronic PHI via the MIHIN in the performance of their jobs.
2. It is the responsibility of the Participant to ensure that Authorized Users are appropriately trained and use workstations in a secure and legitimate manner, and only as permitted by the Participant's computer security policies.
3. It is the responsibility of the Participant to ensure that workstations that are permitted to access the MIHIN are located in an area that can be secured when Authorized Users are not in the work area that contains the workstation.
4. Participants shall ensure that, when practicable, the unattended workstation will be turned off, have a password-protected or other secure screen saver, or utilize an automatic logoff mechanism.
5. Authorized Users may access electronic PHI only for which they have been authorized. Participant is responsible for ensuring that Authorized Users are granted access to electronic PHI based on the job requirements for that Authorized User.
6. E-mail to external destinations should not contain PHI unless it complies with the policies, procedures, encryption or other security requirements of Participant, consistent with HIPAA.
7. The Executive Committee is responsible for ensuring that MIHIN staff and vendors maintain the security of the hardware used in the system, control physical access to facilities where the hardware is located, and comply with all applicable laws and regulations governing system security including at a minimum, HIPAA standards pertaining to system and workstation security.

References:

1. 45 CFR Parts 160 and 164: Health Insurance Reform: Security Standards; Final Regulations.
2. National Institute of Standards and Technology, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

MIHIN Security Policy 005: Termination Procedure

Policy:

As appropriate, the MIHIN and its Participants shall implement procedures for terminating access to electronic PHI in the RHIO's Systems when the employment of an Authorized User ends.

Procedure:

1. The following actions will be performed by Participant or RHIO, as applicable, when the employment of a Authorized User ends ("Terminated Employee") for whatever reason:
 - If the Terminated Employee works for a Participant, the Participant shall notify the RHIO or otherwise disable Terminated Employees access to electronic PHI as soon as practicable, but in no event in longer than twelve (12) hours of employee's termination, if involuntary or if voluntary but concerns regarding security reasonably arise (for example, a disaffected employee).
 - If the Terminated Employee works for a Participant, the Participant shall notify the RHIO or otherwise disable Terminated Employees access to electronic PHI in the RHIO no later than twenty-four (24) hours upon employee leaving employment, if voluntary and amicable.
 - If the Terminated Employee worked for the RHIO, the RHIO shall disable access to electronic PHI within the same parameters as set forth above for Participants
 - If the cause of termination was a violation of confidentiality or security policies, the Participant employer of the Terminated Employee shall conduct the required notifications without delay.
 - It is the responsibility of the Participant employer of the Terminated Employee to ensure that the Terminated Employee cannot damage any information systems.
2. The RHIO or the Participant, as applicable, will ensure that all physical access mechanisms that the terminated Authorized User was in possession of are returned or disabled. Such mechanisms may include:
 - Keys to areas that contain electronic PHI.
 - Access codes to keyless doors.
3. When appropriate and feasible, the Participant or the RHIO, as applicable, will perform an exit interview to address security concerns.
4. The RHIO or the Participant, as applicable, will be responsible for completion of documentation relating to termination. Such documentation shall be maintained for at least six (6) years.

References:

1. 45 CFR Parts 160 and 164: Health Insurance Reform: Security Standards; Final Regulations.
2. National Institute of Standards and Technology, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

MIHIN Security Policy 006: Response and Reporting

Policy:

The RHIO and the Participants will identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known or reasonably anticipated; and document security incident investigations and their outcomes.

Procedure:

1. Whenever a security incident is suspected or confirmed, the incident shall be evaluated and, if material, reported by the Security officer. Incident response procedures for detection, reporting, documentation, and resolution will be followed. Examples of possible security incidents include a virus, worm, hoax e-mail, notification from a Business Associate, discovery of hacking tools, misdirected e-mail, or altered data.
2. Authorized Users shall be trained on information systems security, including social engineering and attacks such as phishing. A means for reporting attempts at social engineering shall be developed.
3. Upon discovery of a security incident, the discovering party shall:
 - Evaluate the type and scope of security incident, and evaluate the probability that data was inappropriately accessed.
 - Initiate the appropriate response.
 - Determine physical and electronic evidence to be gathered as part of the incident investigation.
 - Monitor that any damage from a security incident is repaired or mitigated and that the vulnerability is eliminated or minimized where possible.
 - Initiate, complete, and document the incident investigation.
 - Communicate new issues or vulnerabilities to the system vendor or other parties as applicable, and work to eliminate or mitigate the vulnerability.
4. In the event that the MIHIN discovers the security incident, it shall notify the appropriate Participant (s) in a timely manner and in accordance with the terms of this policy.
5. Participant(s) will determine if notification to affected patients should be made, subject to any applicable state security breach notification laws.
6. Authorized Users having access to electronic PHI in the MIHIN will receive training on the incident reporting and response process.

References:

1. 45 CFR Parts 160 and 164: Health Insurance Reform: Security Standards; Final Regulations.
2. National Institute of Standards and Technology, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

MiHIN Privacy and Security Sub-WorkGroup

	Privacy Challenges to HIE within the State of Michigan 	Rank Difficulty to Overcome (1 to 10 Scale) (1 = not very; 10 = extremely) Why?	Identify ways to mitigate or eliminate the challenge.	List Groups that are impacted (Consumers, Providers, Insurers, Government, Other?)
1				
2				
3				
4				
5				
	Security Challenges to HIE within the State of Michigan 	Rank Difficulty to Overcome (1 to 10 Scale) (1 = not very; 10 = extremely) Why?	Identify ways to mitigate or eliminate the challenge.	List Groups that are impacted (Consumers, Providers, Insurers, Government, Other?)
1				
2				
3				
4				
5				

MiHIN Privacy and Security Sub-WorkGroup

Privacy Challenges to HIE between Michigan and other States  	Rank Difficulty to Overcome (1 to 10 Scale) (1 = not very; 10 = extremely) Why?	Identify ways to mitigate or eliminate the challenge.	List Groups that are impacted (Consumers, Providers, Insurers, Government, Other?)
1			
2			
3			
4			
5			
Security Challenges to HIE between Michigan and Other States 	Rank Difficulty to Overcome (1 to 10 Scale) (1 = not very; 10 = extremely) Why?	Identify ways to mitigate or eliminate the challenge.	List Groups that are impacted (Consumers, Providers, Insurers, Government, Other?)
1			
2			
3			
4			
5			